

456-TP-015-001

EOSDIS Core System Project

Mission Operation Procedures for the Pre-Release B Testbed for the ECS Project

May 1997

Hughes Information Technology Systems
Upper Marlboro, Maryland

Mission Operation Procedures for the Pre-Release B Testbed for the ECS Project

May 1997

Prepared Under Contract NAS5-60000

APPROVED BY

William E. Burford, Site Manager
EOSDIS Core System Project

Date

Hughes Information Technology Systems
Upper Marlboro, Maryland

456-TP-015-001

This page intentionally left blank.

Preface

This document is a contract deliverable with an approval code of 3. This technical paper is delivered to NASA for information only, but is subject to approval as meeting contractual requirements.

Any questions should be addressed to:

GDAAC Performance Analyst
ECS Project / GSFC
Hughes Information Technology Systems
1616 McCormick Drive
Upper Marlboro, MD 20774

DISCLAIMER: This publication is used as a preliminary operations guide to describe the existence/capabilities, totally or partially, of the software tools on the GDAAC Pre-Release B Testbed. These tools may or may not conform to the Pre-Release B Testbed Implementation Plan for the ECS Project. Investigation or use of existing tools not in the Plan is not encouraged, unsupported and done so to the peril of the user.

This page intentionally left blank.

Abstract

This document, The Mission Operation Procedures for the GDAAC Pre-Release B Testbed for ECS, provides DAAC procedures that assign and describe operators, engineers, operations support, administration and management staff actions required to configure, maintain and operate the Pre-Release B ECS system. The DAAC portion of this document contains standard procedures that can be modified at the DAACs during subsequent training, operations exercises and procedure review activities to reflect desired uniqueness. The objectives of the Release A system are to provide ECS components to support the MODIS mission; Version 0 Data Access; EOS-AM-1 and Landsat 7 Interface Testing; and EOS-AM- 1 Algorithm Integration and Test.

Keywords: operations, DAACs, SMC, EOC, mission support, operation procedures, TRMM, EOS, AM-1, Landsat 7, software, integration, test, SSI&T, Version 0

This page intentionally left blank.

Change Information Page

List of Effective Pages			
Page Number		Issue	
Title		Original	
iii through xxxii		Original	
1-1 through 1-4		Original	
2-1 through 2-4		Original	
3-1 through 3-90		Original	
4-1 through 4-18		Original	
5-1 through 5-16		Original	
6-1 through 6-16		Original	
7-1 through 7-16		Original	
8-1 through 8-20		Original	
9-1 through 9-92		Original	
10-1 through 10-4		Original	
11-1 through 11-54		Original	
12-1 through 12-14		Original	
13-1 through 13-16		Original	
14-1 through 14-22		Original	
15-1 through 15-6		Original	
Document History			
Document Number	Status/Issue	Publication Date	CCR Number
456-TP-015-001	Original	May 1997	

Change Information Page (continued)

List of Effective Pages			
Page Number		Issue	
16-1 through 16-2		Original	
17-1 through 17-2		Original	
18-1 through 18-2		Original	
19-1 through 19-46		Original	
20-1 through 20-2		Original	
21-1 through 21-12		Original	
22-1 through 22-40		Original	
23-1 through 23-10		Original	
24-1 through 24-2		Original	
25-1 through 25-4		Original	
26-1 through 26-6		Original	
A-1 through A-2		Original	
AB-1 through AB-11		Original	
Document History			
Document Number	Status/Issue	Publication Date	CCR Number
456-TP-015-001	Original	May 1997	

Contents

Preface

Abstract

1. Introduction

1.1 Identification	1-1
1.2 Scope	1-1
1.3 Purpose	1-1
1.4 Status and Schedule.....	1-1
1.5 Organization	1-2

2. Related Documentation

2.1 Parent Documents.....	2-1
2.2 Applicable Documents	2-1
2.3 Information Documents.....	2-4
2.3.1 Information Documents Referenced	2-4
2.3.2 Information Documents Not Referenced	2-4

3. System Administration

3.1 System Startup and Shutdown.....	3-1
3.1.1 Startup	3-1
3.1.2 Shutdown.....	3-4
3.2 System Backup and Restore.....	3-9
3.2.1 Incremental Backup.....	3-9
3.2.2 Full Backup	3-13
3.2.3 File Restore.....	3-16
3.2.4 Complete System Restore	3-19
3.2.5 Tape Handling.....	3-23

3.3 System Log Maintenance	3-28
3.4 User Administration	3-30
3.4.1 Adding a User.....	3-30
3.4.2 Deleting a User.....	3-34
3.4.3 Changing a User Account Configuration	3-37
3.4.4 Changing User Access Privileges.....	3-41
3.4.5 Changing a User Password.....	3-44
3.4.6 Checking a File/Directory Access Privilege Status.....	3-47
3.4.7 Changing a File/Directory Access Privilege	3-50
3.4.8 Moving a User's Home Directory.....	3-52
3.5 Installing a New Workstation.....	3-55
3.5.1 Preparation.....	3-56
3.5.2 Installation.....	3-58
3.5.3 Testing and Verification.....	3-74
3.6 DCE Configuration.....	3-79
3.6.1 Configuring Initial Cell.....	3-79
3.6.2 Configuring DTS Servers.....	3-82
3.6.3 Configuring Additional CDS Servers.....	3-83
3.6.4 Configuring Security and CDS Client Systems	3-85
3.6.5 Configuring DTS Clerks	3-86
3.6.6 Configuring GDA Servers.....	3-87
3.6.7 Creating Security Server Replica	3-88
3.6.8 Unconfiguring DCE Client.....	3-89

4. Database Administration

4.1 The Role of the Database Administrator (DBA).....	4-1
4.2 Conventions, SQL Server Nomenclature, and Directory Structure	4-1
4.3 SQL Server Installation.....	4-3
4.4 DBA Functions.....	4-4
4.4.1 Starting, Stopping, and Showing the Server(s)	4-5
4.4.2 Creating Logical Devices	4-5
4.4.3 Creating and Altering Databases.....	4-6
4.4.4 Data Placement - Segmentation	4-7

4.4.5 Monitoring Space Usage	4-8
4.4.6 Creating Database Objects	4-9
4.4.7 Creating and Managing Users Logins	4-10
4.4.8 Permissions	4-11
4.5 Backup and Recovery	4-11
4.5.1 Automatic Backups	4-12
4.5.2 Manual Backups	4-13
4.5.3 Manual Recovery	4-13
4.5.4 The BulkCopy Utility	4-13
4.6 Database Performance and Tuning	4-15
4.7 Installation of the pdps Application	4-16
4.7.1 Installation Scripts for the pdps Application Database	4-16
4.7.2 The AUTOSYS Application and other Configuration Issues	4-17

5. Security Services

5.1 Generating Security Reports	5-2
5.2 Running the Network Authentication Service	5-2
5.3 Monitoring Network Vulnerabilities	5-4
5.4 Ensuring Password Integrity	5-5
5.4.1 Detecting Weak Passwords	5-5
5.4.2 Enforcing Strong Passwords	5-10
5.5 Monitoring Requests for Network Services	5-12
5.6 Monitoring File and Directory Integrity	5-13
5.6.1 Updating the Tripwire Database	5-14
5.6.2 Configuring the tw.config file	5-15
5.7 Reporting Security Breaches	5-15
5.8 Initiating Recovery from Security Breaches	5-15

6. Network Administration

6.1 HP Open View Network Node Manager (NNM).....	6-1
6.1.1 Starting Network Node Manager (NNM)	6-2
6.1.2 Creating Additional Objects.....	6-3
6.1.3 Viewing the Current Network and System Configuration	6-10
6.1.4 Viewing Network Address Information.....	6-11
6.1.5 Viewing How Traffic is Routed on a Network	6-13
6.1.6 Viewing the Services Available on a Node.....	6-14
6.2 Diagnosing Network Problems	6-15

7. System Monitoring

7.1 Checking the Health and Status of the Network	7-1
7.1.1 Starting NNM (Network Node Manager)	7-2
7.1.2 Verify That an Object Is Not Functioning.....	7-3
7.1.3 Looking at Maps for Color Alerts	7-4
7.1.4 Looking at Maps for New Nodes	7-5
7.1.5 Creating Special Submaps for Monitoring Status	7-5
7.1.6 Checking for Event Notifications.....	7-6
7.1.7 Rediscovering the Network.....	7-7
7.2 Tivoli Enterprise Console.....	7-8

8. Problem Management

8.1 Problem Resolution Process — An Overview	8-1
8.2 Using the Trouble Ticket System Tool	8-7
8.2.1 Accessing the Trouble Ticket System.....	8-8
8.2.2 Submit a Trouble Ticket.....	8-11
8.2.3 Reviewing and Modifying Open Trouble Tickets.....	8-13
8.2.4 Forwarding Trouble Tickets.....	8-14

8.2.5 Adding Users to Remedy	8-15
8.2.6 Changing Privileges in Remedy	8-15
8.2.7 Modifying Remedy's Configuration.....	8-16
8.2.8 Generating Trouble Ticket Reports.....	8-16
8.2.9 Re-prioritization of Dated Trouble Ticket Logs.....	8-16
8.3 Using Hypertext Mark-up Language (HTML) Screens	8-17
8.3.1 ECS Trouble Ticketing HTML Submit Screen.....	8-17
8.3.2 ECS Trouble Ticketing HTML Success Screen.....	8-18
8.3.3 ECS Trouble Ticketing HTML List Screen	8-18
8.3.4 ECS Trouble Ticketing HTML Detailed Screen.....	8-18
8.3.5 ECS Trouble Ticketing HTML Help Screen.....	8-19
8.4 Emergency Fixes	8-20

9. Configuration Management

9.1 Configuration Identification Procedure.....	9-1
9.1.1 Purpose	9-1
9.1.2 Applicable to	9-2
9.1.3 References	9-2
9.1.4 Procedures	9-2
9.2 Configuration Change Control Procedures	9-3
9.2.1 Purpose	9-3
9.2.2 GDAAC Testbed Change Control Board (GTCCB) Charter.....	9-3
9.2.3 References	9-6
9.2.4 Procedures	9-6
9.3 Configuration Status Accounting Procedures	9-21
9.3.1 Purpose	9-21
9.3.2 Applicable to	9-21
9.3.3 References	9-21
9.3.4 Procedures	9-21

9.4 Archiving Procedures for the SW CM Manager (ClearCase).....	9-22
9.4.1 Purpose	9-22
9.4.2 Applicable to	9-22
9.4.3 References	9-22
9.4.4 Procedures	9-23
9.5 SW Transfer and Installation.....	9-26
9.5.1 Purpose	9-26
9.5.2 Applicable to	9-26
9.5.3 References	9-26
9.5.4 Procedures	9-26
9.6 Change Request Manager.....	9-38
9.6.1 Configuration Change Request (CCR).....	9-39
9.6.2 Accessing Change Request Manager	9-42
9.6.3 View a CCR.....	9-43
9.6.4 Submit a CCR.....	9-43
9.6.5 Change State of CCR	9-45
9.6.6 Modify CCR.....	9-50
9.6.7 Print CCR	9-51
9.6.8 Required Operating Environment	9-52
9.6.9 Reports.....	9-53
9.7 SW Transfer and Installation.....	9-57
9.7.1 Purpose	9-57
9.7.2 Applicable to	9-57
9.7.3 References	9-57
9.7.4 Procedures	9-58
9.8 Change Request Manager.....	9-69
9.8.1 Configuration Change Request (CCR).....	9-70
9.8.2 Accessing Change Request Manager	9-73
9.8.3 View a CCR.....	9-74
9.8.4 Submit a CCR.....	9-74

9.8.5 Change State of CCR	9-76
9.8.6 Modify CCR.....	9-81
9.8.7 Print CCR	9-82
9.8.8 Required Operating Environment	9-83
9.8.9 Reports.....	9-84
9.9 Use of the Baseline Manager.....	9-88
9.9.1 Purpose	9-88
9.9.2 Applicable to	9-89
9.9.3 References	9-89
9.9.4 Procedures	9-89

10. Metadata Administration

10.1 Establishing Collections.....	10-1
10.1.1 Population of Collection-level Metadata.....	10-2
10.1.2 Population of Granule-level Metadata	10-2
10.1.3 Population of Product-specific Metadata	10-2
10.1.4 Specifying ESDT Services	10-3
10.2 Installing ESDTs	10-3
10.2.1 Assembling an ESDT Descriptor	10-3
10.2.2 Inserting the ESDT Descriptor and DLL	10-3
10.3 Maintaining Metadata.....	10-3

11. SSI&T Operational Procedures

11.1 Preparation.....	11-2
11.1.1 Creating a New Earth Science Data Type (ESDT)	11-2
11.1.2 Validating Granule Level Metadata	11-2
11.1.3 Installing an Earth Science Data Type (ESDT) on the Data Server.....	11-2
11.1.4 Validating Successful ESDT Installation.....	11-2
11.1.5 Creating Metadata Configuration Files (MCF'.....	11-2
11.2 Acquiring the Delivered Algorithm Package (DAP)	11-2
11.2.1 Registering a Subscription for a DAP	11-2

11.2.2 Notification of DAP Arrival.....	11-2
11.2.3 Acquiring a DAP from Data Server	11-2
11.2.4 Acquiring a DAP via FTP	11-2
11.3 Configuration Management.....	11-2
11.3.1 Creating and Using a View in ClearCase.....	11-2
11.3.2 Importing Multiple Files into ClearCase from a Directory Structure	11-4
11.3.3 Entering a Single File into ClearCase	11-5
11.3.4 Entering a New Directory into ClearCase.....	11-6
11.3.5 Checking Out an Element from ClearCase	11-7
11.3.6 Checking a Revised Element into ClearCase	11-7
11.3.7 Applying Labels to ClearCase Elements.....	11-8
11.4 SSIT Manager GUI	11-8
11.4.1 General Setup of the SSIT Manager.....	11-8
11.4.2 Setup of Checklist for SSIT Manager	11-11
11.4.3 Running the SSIT Manager for the First Time.....	11-12
11.4.4 Routine Running of the SSIT Manager.....	11-14
11.5 Standards Checking.....	11-15
11.5.1 Checking ESDIS Standards Compliance: FORTRAN 77.....	11-15
11.5.2 Checking ESDIS Standards Compliance: Fortran 90.....	11-18
11.5.3 Checking ESDIS Standards Compliance: C.....	11-18
11.5.4 Checking ESDIS Standards Compliance: Ada.....	11-20
11.5.5 Prohibited Function Checker.....	11-21
11.5.6 Checking Process Control Files	11-22
11.5.7 Extracting Prologs	11-23
11.6 Compiling and Linking	11-23
11.6.1 Updating the Process Control File (PCF).....	11-23
11.6.2 Compiling Status Message Facility (SMF) Files	11-27
11.6.3 Setting up a SDP Toolkit Environment.....	11-30
11.6.4 Compiling a PGE and Linking With SCF Version of SDP Toolkit.....	11-33
11.6.5 Compiling a PGE and Linking with DAAC Version of SDP Toolkit.....	11-36
11.7 Running a PGE in a Simulated SCF Environment at the DAAC.....	11-39
11.7.1 Setting Up the Environment for Running the PGE.....	11-39
11.7.2 Running and Profiling the PGE.....	11-39

11.8	Updating the PDPS Database and Data Server	11-39
11.8.1	Updating the Science Metadata in the PDPS Database.....	11-39
11.8.2	Updating the ESDT Metadata in the PDPS Database.....	11-39
11.8.3	Updating the Operational Metadata in the PDPS Database	11-39
11.8.4	Inserting Test Data Files Into the Data Server	11-39
11.8.5	Inserting Static Files into the Data Server.....	11-39
11.8.6	Inserting the Science Software Executable Package (SSEP) into the Data Server.....	11-39
11.9	PGE Planning and Processing.....	11-39
11.9.1	Using the Planning Workbench.....	11-39
11.9.2	Using the Production Request Editor	11-39
11.9.3	Registering a Subscription for Test Output Files	11-39
11.9.4	Monitoring Production	11-39
11.9.5	Acquiring the Test Output Files from the Data Server	11-39
11.10	File Comparison	11-39
11.10.1	Using the HDF File Comparison Tool GUI.....	11-39
11.10.2	Using theHDF File Comparison Tool hdiff	11-40
11.10.3	Using the ASCII File Comparison Tool.....	11-40
11.10.4	Using the Binary File Comparison Tool	11-41
11.11	Data Visualization.....	11-42
11.11.1	Viewing Product-Created Metadata Using the EOSView Tool.....	11-42
11.11.2	Viewing Product Data with the EOSView Tool	11-44
11.11.3	Viewing Product Data with the IDL Tools	11-44
11.12	Post-Testing Activities	11-44
11.12.1	Validating Inventory/Granule Metadata Updates to the Data Server Database	11-44
11.12.2	promoting the PGE from Test to Production.....	11-44
11.12.3	Reporting Science Software Problems.....	11-44
11.12.4	Reporting ECS Software Problems.....	11-44
11.13	Science Software Archive Package (SSAP).....	11-44
11.13.1	Assembling Components of the SSAP.....	11-44
11.13.2	Creating and Inserting the SSAP into the Data Server.....	11-44

11.14	Troubleshooting and General Investigation	11-44
11.14.1	Examining PGE-Produced Log Files	11-44
11.14.2	Examining the MSS Log File.....	11-48
11.14.3	Using PDPS Prototype-Related Scripts and Examining Message Files.....	11-49
11.15	Miscellaneous.....	11-54
11.15.1	Setting Up the Release A Bulletin Board Service.....	11-54
11.15.2	Obtaining Information from the Bulletin Board Service.....	11-54
11.15.3	Posting Information to the Bulletin Board Service	11-54

12. Resource Planning

12.1	Resource Planning Process.....	12-1
12.2	Resource Planning Workbench Utility.....	12-2
12.2.1	Create a Resource Reservation Request.....	12-3
12.2.2	Edit a Resource Reservation Request.....	12-6
12.2.3	Validate or Reject a Resource Reservation Request	12-7
12.2.4	Approve a Resource Reservation Request	12-7
12.2.5	Commit a Resource Reservation Request	12-8
12.2.6	Resource Planning Reports	12-8
12.2.7	Review Resource Timeline	12-9
12.2.8	Delete a Resource Reservation Request.....	12-9
12.3	Resource Definition Tool	12-10
12.3.1	Add a Resource	12-10
12.3.2	Modify a Resource	12-12
12.3.3	Delete a Resource.....	12-12
12.3.4	Synchronize Resource Listings	12-13

13. Production Planning

13.1	Production Request Editor.....	13-1
13.1.1	Launching the Production Request Editor.....	13-1
13.1.2	Create New Production Request.....	13-2
13.1.3	Edit/Modify Production Request.....	13-4
13.1.4	Review Data Production Requests	13-6
13.1.5	Reports.....	13-8

13.2 Production Planning Workbench.....	13-12
13.1.1 Launching the Planning Workbench and Planning Timeline.....	13-12
13.2.1 Create New Production Plan	13-13
13.2.2 Review Plan Timeline	13-15

14. Production Processing

14.1 Configure AutoSys.....	14-2
14.1.1 AutoSys Runtime Options.....	14-2
14.1.2 Configure Hardware Groups	14-4
14.2 Review Hardware Status	14-5
14.2.1 Review Hardware Status	14-5
14.2.2 Hardware Status View Options	14-6
14.3 Review DPR Dependencies.....	14-7
14.4 Review DPR Production Timeline.....	14-8
14.5 Modify Job Priority	14-9
14.6 Review Alarms.....	14-10
14.6.1 Review Alarms.....	14-10
14.6.2 Alarm Selection Configuration	14-11
14.7 Review Job Activities.....	14-12
14.7.1 Review Job Activities.....	14-12
14.7.2 Review Job Selection Criteria.....	14-13
14.8 Modify Job Status.....	14-14
14.9 Activity Log	14-16
14.10 Job Dependency Log.....	14-17
14.11 Defining Monitors/Browser	14-18
14.11.1 Defining Monitors/Browser	14-18
14.11.2 Monitor/Browser Reports.....	14-19
14.12 Database Maintenance Time Change.....	14-20
14.13 Production Reports.....	14-20
14.13.1 AutoSys Reports.....	14-21

15. Quality Assurance

15.1 Launching the QA Monitor GUI.....	15-1
15.2 DAAC Product QA	15-2
15.3 Product History.....	15-4
15.4 EOSView.....	15-5

16. Ingest

17. Archive

18. Data Distribution

19. User Services

19.1 ECS User Account Management.....	19-1
19.1.1 Retrieve User Account/Validate a User	19-1
19.1.2 Create a User Account.....	19-2
19.1.3 Account Creation from URL Registration	19-11
19.1.4 Edit/Modify an Existing Account.....	19-13
19.1.5 Deleting an ECS Account.....	19-22
19.1.6 Canceling an ECS Account.....	19-23
19.1.7 Changing an ECS User's Password.....	19-25
19.2 Processing an Order.....	19-27
19.2.1 Create a User Contact Log Record.....	19-27
19.2.2 Retrieve User Information.....	19-32
19.2.3 Locate Data Via Search and Order Tool	19-33
19.2.4 Request Price Estimate.....	19-35
19.2.5 Specify Order Details	19-36
19.2.6 Update User Contact Log.....	19-36
19.3 Cancel an Order.....	19-38
19.3.1 ECS Order Tracking.....	19-39
19.3.2 Cancel an Order Via Data Server Subsystem.....	19-41

19.4 Fulfilling a Subscription.....	19-42
19.4.1 Fulfilling a One-Time Subscription	19-43
19.4.2 Fulfilling an Open Ended Subscription.....	19-43
19.4.3 Returning a List of Subscriptions.....	19-44
19.4.4 Editing or Canceling a Subscription.....	19-44
19.5 Cross-DAAC Referral Process.....	19-45
19.6 Guide Authoring and Maintenance	19-46

20. Library Administration

20.1 SEO Document Maintenance	20-1
20.1.1 Authoring Documents	20-1
20.1.2 Formatting Documents.....	20-1
20.1.3 Importing Documents.....	20-1
20.1.4 Exporting Documents.....	20-1
20.1.5 Metadata Maintenance	20-1
20.2 On-Site Document Maintenance	20-1
20.2.1 Authoring Documents	20-1
20.2.2 Importing Documents.....	20-1
20.2.3 Formatting Documents.....	20-1
20.2.4 Searching for a Document.....	20-1
20.2.5 Metadata Maintenance	20-1
20.3 Preparing Documents for Insertion into the DDSRV.....	20-1
20.4 Maintenance of Document Inventory Records and Links to Configuration Items in Baseline Manager.....	20-1
20.5 Document Metadata Insertion Subscription.....	20-1
20.6 Document Repository Maintenance	20-1
20.7 Document Access Control.....	20-1
20.8 Retrieval of HTTP Formatted Documents	20-1

21. COTS Hardware Maintenance

21.1	COTS Hardware Support - General	21-1
21.1.1	Corrective Maintenance	21-1
21.1.2	Preventive Maintenance	21-2
21.1.3	Configuration Management.....	21-2
21.1.4	COTS Hardware Support Safety	21-2
21.2	COTS Hardware Support - Contract Information.....	21-2
21.2.1	Management of COTS Hardware Support Contracts.....	21-3
21.2.2	Contract Maintenance Terms	21-3
21.2.3	COTS Hardware Database	21-4
21.3	Hardware Repairs - Standard	21-6
21.3.1	Hardware Problem Reporting.....	21-6
21.3.2	Initial Troubleshooting/Diagnostics.....	21-7
21.3.3	Hardware Corrective Maintenance Actions	21-7
21.3.4	Contract On-Site Hardware Support	21-8
21.3.5	Return-to-Depot Support.....	21-10
21.4	Maintenance Spares.....	21-10
21.4.1	Installed Maintenance Spares.....	21-11
21.4.2	Use of Maintenance Spares	21-11
21.4.3	Return of Failed LRUs	21-11
21.5	Non-standard Hardware Support.....	21-12
21.5.1	Escalation of COTS Hardware Support Problem.....	21-12
21.5.2	Time and Material (T&M) Hardware Support.....	21-12

22. Software Maintenance

22.1	COTS Software Maintenance.....	22-2
22.1.1	Management of COTS Software Maintenance Contracts	22-3
22.1.2	Management of COTS Software Licenses	22-3
22.1.3	COTS Software Installation	22-3
22.1.4	Obtaining COTS Software Support.....	22-4

22.2 Custom Software Maintenance	22-7
22.2.1 Implementation of Modifications	22-9
22.2.2 Test Plans and Procedures	22-10
22.2.3 Custom Software Installation	22-12
22.2.4 Obtaining Software Support	22-37
22.2.5 Science Software	22-39

23. Property Management

23.1 Receipt of Equipment and Software	23-2
23.2 Equipment Tagging	23-3
23.3 Property Records and Reporting	23-4
23.3.1 Maintaining Property Records	23-5
23.3.2 Property Reporting	23-5
23.3.3 Reporting Loss, Theft, Damage or Destruction	23-6
23.3.4 Obtaining Relief from Accountability	23-6
23.4 Equipment Relocation	23-6
23.4.1 Intra-site Relocation	23-6
23.4.2 Inter-site Relocation	23-7
23.4.3 Relocation Off-site for Vendor Repairs	23-7
23.4.4 External Transfers	23-7
23.5 Inventories and Audits	23-7
23.6 Storage	23-8
23.6.1 Segregation Requirements	23-8
23.6.2 Stock Rotation	23-8
23.6.3 Physical Security	23-9
23.7 Packing and Shipping	23-9

24. Installation Planning

24.1 Responsibilities	23-1
24.2 Process Description.....	23-1
24.3 Maintenance of Facility and Network Diagrams	23-2
24.4 Maintenance of LAN Cable Management Schema.....	23-2

25. COTS Training

25.1 Requesting COTS Training.....	23-1
25.2 Coordinating COTS Training.....	23-2
25.3 Canceling/Rescheduling COTS Training.....	23-3
25.4 Maintenance of COTS Training Records.....	23-3
25.5 Contractor COTS Training Funds Accounting	23-4

26. Interoperability Subsystem Administration

26.1 Accessing ESOD	23-2
26.2 ESOD Moderation.....	23-3
26.3 ESOD Administration	23-4
26.3.1 Create a Moderation Group.....	23-4
26.3.2 Update a Moderation Group.....	23-5
26.3.3 Delete a Moderation Group.....	23-6

List of Figures

8.1-1. ECS Problem Management Concept - Part I	8-5
8.1-2. ECS Problem Management Concept - Part II.....	8-6
8.2-1. Trouble Ticket E-mail Template.....	8-13
9.2.4-1. ECS Configuration Change Request (CCR).....	9-7
9.2.4-2: ECS CCR Impact Analysis	9-11
9.2.4-3 ECS M&O CCR Impact Summary	9-12

9.2.4-5 Work-Flow Diagram for Site-level CM Administrator	9-16
9.2.4-6 Deviation/ Waiver Form	9-20
9.5.4-1 SW Transfer Functional Flow.....	9-28
9.5.4-2 SW Installation Functional Flow	9-29
9.5.4-3 Detailed Points of View	9-31
9.5.4-4 Detailed Points of View	9-32
9.5.4-5 Detailed Points of View	9-33
9.7.4-1 SW Transfer Functional Flow.....	9-59
9.7.4-2 SW Installation Functional Flow	9-60
9.7.4-3 Detailed Points of View	9-62
9.7.4-4 Detailed Points of View	9-63
9.7.4-5 Detailed Points of View	9-64
14.1-1. AutoSys Hardware Group File Example	14-4
14.9-1. Sample Activity Log.....	14-16
14.10-1. Sample Job Dependency Log.....	14-17
14.11-1. Sample Browser Screen	14-18

List of Tables

3.1-1. Startup/Shutdown - Activity Checklist.....	3-1
3.1-2. Cold System Startup - Quick-Step Procedures	3-3
3.1-3. Warm System Startup - Quick-Step Procedures	3-4
3.1-4. Normal System Shutdown - Quick-Step Procedures	3-6
3.1-5. Emergency System Shutdown - Quick-Step Procedures	3-9
3.1-6. Server System Shutdown - Quick-Step Procedures.....	3-9
3.2-1. Incremental Backup - Activity Checklist.....	3-10
3.2-2. Perform Incremental Backup - Quick-Step Procedures.....	3-12
3.2-3. Full Backup - Activity Checklist	3-13
3.2-4. Perform Full Backup - Quick-Step Procedures.....	3-15
3.2-5. File Restore - Activity Checklist.....	3-16

3.2-6. Restore a File - Quick-Step Procedures	3-18
3.2-7. Complete System Restore - Activity Checklist.....	3-19
3.2-8. Restore a Partition - Quick-Step Procedures.....	3-22
3.2-9. Indexing Tapes - Activity Checklist	3-23
3.2-10. Index Tapes - Quick-Step Procedures.....	3-25
3.2-11. Labeling Tapes - Activity Checklist	3-26
3.2-12. Label Tapes - Quick-Step Procedures.....	3-28
3.3-1. System Log Maintenance - Quick-Step Procedures	3-30
3.4-1. Adding a User - Activity Checklist.....	3-31
3.4-2. Add New User - Quick-Step Procedures	3-33
3.4-3. Deleting a User - Activity Checklist.....	3-34
3.4-4. Delete a User - Quick-Step Procedures.....	3-36
3.4-5. Change a User Account Configuration - Activity Checklist.....	3-37
3.4-6. Change User Account Configuration - Quick-Step Procedures.....	3-40
3.4-7. Changing User Access Privileges - Activity Checklist.....	3-41
3.4-8. Change User Access Privileges - Quick-Step Procedures	3-44
3.4-9. Changing a User Password - Activity Checklist.....	3-45
3.4-10. Change User Password - Quick-Step Procedures	3-47
3.4-11. Checking a File/Directory Access Privilege Status - Activity Checklist.....	3-47
3.4-12. Check a File/Directory Access Privilege Status - Quick-Step Procedures	3-49
3.4-13. Changing a File/Directory Access Privilege - Activity Checklist	3-50
3.4-14. Change a File/Directory Access Privilege - Quick-Step Procedures.....	3-52
3.4-15. Moving a User's Home Directory - Activity Checklist.....	3-53
3.4-16. Move a User's Home Directory - Quick-Step Procedures.....	3-55
3.5-1. Installing a New Workstation - Activity Checklist.....	3-56
3.5-2. Hardware Preparation - Activity Checklist.....	3-56
3.5-3. Prepare for Network Configuration - Quick-Step Procedures	3-57
3.5-4. Report to Inventory - Quick-Step Procedures.....	3-58
3.5-5. Install the Solaris 2.4 Operating System - Quick-Step Procedures.....	3-61

3.5-6. Install the HP-UX 9.05 Operating System - Quick-Step Procedures	3-64
3.5-7. Install the IRIX 5.3 or 6.2 Operating System - Quick-Step Procedures	3-67
3.5-8. Configure the NCD - Quick-Step Procedures.....	3-71
3.5-9. Install Custom Software - Quick-Step Procedures	3-73
3.5-10. Install COTS Software - Quick-Step Procedures.....	3-74
3.5-11. Reboot - Quick-Step Procedures.....	3-75
3.5-12. Reboot the NCD - Quick-Step Procedures	3-76
3.5-13. Log In - Quick-Step Procedures.....	3-77
3.5-14. Test Environment - Activity Checklist	3-78
3.5-15. Test Environment - Quick-Step Procedures.....	3-79
3.6-1. Configuring Initial Cell - Quick-Step Procedures.....	3-81
3.6-2. Configuring DTS Servers - Quick-Step Procedures	3-83
3.6-3. Configuring Additional CDS Servers - Quick-Step Procedures.....	3-85
3.6-4. Configuring Security and CDS Client Systems - Quick-Step Procedures.....	3-86
3.6-5. Configuring DTS Clerks - Quick-Step Procedures.....	3-87
3.6-6. Configuring GDA Servers - Quick-Step Procedures	3-88
3.6-7. Creating a Security Server Replica - Quick-Step Procedures.....	3-89
3.6-8. Unconfiguring DCE Client - Quick-Step Procedures.....	3-90
4.2-1. SQL Server General Definitions.....	4-1
4.2-2. SYBASE Directory Structure	4-2
4.3-1. SQL Server Parameters and Options	4-4
4.5-1. Backup and Recovery Definitions	4-12
4.5-2. Automatic Backup Components	4-12
4.7.1-1. Installation Steps for the pdps Application Database	4-16
5-1. Security - Activity Checklist.....	5-1
6.1-1. Network Administration - Activity Checklist.....	6-2
6.1-2. Starting NNM (Network Node Manager) - Quick-Step Procedures.....	6-3
6.1-3. Adding a Network Object - Quick-Step Procedures.....	6-5
6.1-4. Adding a Segment Object- Quick-Step Procedures	6-6

6.1-5. Adding a Node Object- Quick-Step Procedures	6-8
6.1-6. Adding an IP Interface Object- Quick-Step Procedures	6-10
6.1-7. Viewing the Current Network and System Configuration -Quick-Step Procedures	6-11
6.1-8. Viewing Network Address Information- Quick-Step Procedures	6-12
6.1-9. Viewing How Traffic is Routed on a Network- Quick-Step Procedures.....	6-14
6.1-10. Viewing the Services Available on a Node- Quick-Step Procedures	6-15
7.1-1A. Monitoring - Activity Checklist.....	7-1
7.1-1B. Starting NNM - Quick-Step Procedures.....	7-3
7.1-1C. Verify - Quick-Step Procedures	7-4
7.1-2. Color ALerts- Quick-Step Procedures	7-5
7.1-6. Event Notifications - Quick-Step Procedures	7-7
7.1-7. Rediscovery - Quick-Step Procedures	7-8
7.2-1. Disk Event Configuration	7-8
7.2-2 Security Event Configuration.....	7-10
7.2-3. Network Event Configuration.....	7-11
7.2-4. System Event Configuration	7-13
7.2-5 Printer Event Configuration.....	7-14
8.2-1. Trouble Ticket System - Activity Checklist	8-8
8.2-2. Pre-RelB-Trouble Ticket Field Description.....	8-9
8.2-3. Table of Access Control Groupings.....	8-15
8.3-1. Trouble Ticket HTML Submit Screen Field Description	8-17
8.3-2. Trouble Ticket HTML List Screen Field Description	8-18
8.3-3 Trouble Ticket HTML Detailed Screen Field Description	8-19
9.5.4-1. Data Activity for Workflow at the SMC.....	9-34
9.5.4-2A. Data Activity for Workflow at the DAAC.....	9-35
9.5.4-2B. Data Activity for Workflow at the DAAC	9-36
9.5.4-2C. Data Activity for Workflow at the DAAC	9-37
9.6.4-1. Submit Record Field Descriptions	9-44

9.6.4-2. Submit a CCR - Quick-Step Procedures	9-45
9.6-5 Change State of a CCR - Quick-Step Procedures	9-46
9.6.5-1. Assign-Eval Field Descriptions	9-46
9.6.5-2 Assign-Implement Field Descriptions	9-47
9.6.5-3 Assign-Verify Field Descriptions	9-49
9.6.5-4. Verify State Field Descriptions.....	9-49
9.6.5-5. Close State Field Descriptions	9-50
9.6.6. Modify a CCR - Quick-Step Procedures.....	9-51
9.6.7. Print a CCR - Quick-Step Procedures	9-52
9.6.9. Reports.....	9-53
9.7.4-1. Data Activity for Workflow at the SMC.....	9-65
9.7.4-2A. Data Activity for Workflow at the DAAC.....	9-66
9.7.4-2B. Data Activity for Workflow at the DAAC	9-67
9.7.4-2C. Data Activity for Workflow at the DAAC	9-68
9.8.4-1. Submit Record Field Descriptions	9-75
9.8.4-2. Submit a CCR - Quick-Step Procedures	9-76
9.8-5. Change State of a CCR - Quick-Step Procedures.....	9-77
9.8.5-1. Assign-Eval Field Descriptions	9-77
9.8.5-2. Assign-Implement Field Descriptions	9-78
9.8.5-3. Assign-Verify Field Descriptions	9-80
9.8.5-4. Verify State Field Descriptions.....	9-80
9.8.5-5. Close State Field Descriptions	9-81
9.8.6. Modify a CCR - Quick-Step Procedures.....	9-82
9.8.7. Print a CCR - Quick-Step Procedures	9-83
9.8.9. Reports.....	9-84
10.1-1. Metadata Administration - Activity Checklist	10-1
12.1-1. Resource Planning - Activity Checklist.....	12-2
12.2-1. Create a Resource Reservation - Quick-Step Procedures	12-4
12.2-2. Frequency Qualifiers.....	12-6

13.1-1. Production Request - Activity Checklist.....	13-1
13.1-2. Create New Production Request - Quick-Step Procedures.....	13-4
13.1-3. Edit/Modify Production Request - Quick-Step Procedures	13-6
13.1-4. Review Data Production Request - Quick-Step Procedures.....	13-8
13.1-5. Generate Reports - Quick-Step Procedures	13-11
13.1-6. Generate Reports - Quick-Step Procedures	13-11
13.2-1. Production Planning - Activity Checklist	13-12
13.2-2. Create New Production Plan - Quick-Step Procedures.....	13-15
13.2-3. Review Plan Timeline - Quick-Step Procedures.....	13-16
14.1-1. Production Planning - Activity Checklist	14-1
14.1-2. Runtime Options Table.....	14-2
14.13-1. Production Reports - Activity Checklist.....	14-21
14.13-2. AutoSys Reports - Quick-Step Procedures.....	14-22
15.1-1. Quality Assurance - Activity Checklist	15-1
19.1-1. ECS User Account Management - Activity Checklist.....	19-1
19.1-2. Validate a User - Quick-Step Procedures	19-2
19.1-3. Create an ECS User Account - Activity Checklist	19-3
19.1-4. Creating an ECS User Account - Quick-Step Procedures	19-9
19.1-5. Completion of URL Registration - Quick-Step Procedures.....	19-12
19.1-6. Edit/Modify and Existing Account - Activity Checklist.....	19-13
19.1-7. Edit/Modify an Account - Quick-Step Procedures	19-21
19.1-8. Deleting an ECS Account - Quick-Step Procedures.....	19-23
19.1-9. Canceling an ECS Account - Quick-Step Procedures	19-25
19.1-10. Changing an ECS User's Password - Quick-Step Procedures.....	19-26
19.2-1. Processing an Order - Activity Checklist.....	19-27
19.2-2. Creating a User Contact Log - Quick-Step Procedures	19-31
19.2-3. Retrieve User Account - Quick-Step Procedures.....	19-33
19.2-4. Locate Data Via Search & Order Tool - Activity Checklist.....	19-34
19.2-5. Update User Contact Log Record - Quick-Step Procedures.....	19-38

19.3-1. Cancel an Order - Activity Checklist.....	19-39
19.3-2. ECS Order Tracking - Quick-Step Procedure.....	19-40
19.3-3. Cancel an Order Via DSS - Quick-Step Procedure.....	19-42
19.4-1. Fulfilling a Subscriptions - Activity Checklist	19-43
19.4-2. Fulfilling a One-Time Subscription - Quick-Step Procedure	19-43
19.4-3. Fulfilling an Open Ended Subscription - Quick-Step Procedures	19-44
19.4-4. Returning a List of Subscriptions - Quick-Step Procedures	19-44
19.4-5. Editing or Canceling a Subscription - Quick-Step Procedures.....	19-45
21.2-1. Hardware Support Bulletin Board Fields.....	21-3
21.2-2. Maintenance Contractor's Support Terms	21-4
21.2-3. Maintenance Database Fields.....	21-5
21.3-1. Initial Troubleshooting/Diagnostics Procedures.....	21-7
21.3-2. Hardware Corrective Maintenance Actions.....	21-8
21.3-3 Obtaining On-Site Hardware Support.....	21-9
22.1-1. COTS Maintenance - Activity Checklist	22-2
22.2-1. Custom Software Maintenance - Activity Checklist.....	22-8
22.2-2. ECS Software Oriented Tables State Table	22-30
22.2-3. Valid State Transitions.....	22-31
22.2-4. Valid State Assignment Given Current Promotion Level.....	22-32
22.2-5. Science Software Oriented State Table.....	22-33
22.2-6. Science Software Oriented Valid State Transitions.....	22-34
22.2-7. Science Software Oriented Promotion Table.....	22-34
22.2-8. Detailed Steps of SW Installation	22-36
23.1-1. Property Management - Activity Checklist	23-1
25.1-1. COTS Training - Activity Checklist	25-1
26.1-1. IOS Administration - Activity Checklist	26-2

Appendix A. Additional Material

Abbreviations and Acronyms

This page intentionally left blank.

1. Introduction

This document, Mission Operation Procedures for the Pre-Release B Testbed for ECS, provides Maintenance and Operations (M&O) procedures to configure, maintain and operate the Pre-Release B ECS system (MODIS Release).

1.1 Identification

This document meets the milestone specified as Contract Data Requirements List (CDRL) Item 117, DID 611/OP3 under contract NAS5-6000. It reflects the ECS as delivered at Pre-Release B.

1.2 Scope

The scope of this document is directed to DAAC M&O activities to support the Pre-Release B ECS system (MODIS Release). Both procedures and instructions are identified. Operations procedures are defined as the step-by-step commands or on-line procedures needed to perform a function. The Operations Instructions are the off-line procedures or directives for performing administrative, operations, management or operations support activities, e.g., Configuration Management, Problem Management, Performance Reporting, etc. Each DAAC may modify these procedures and instructions to accommodate site-specific M&O requirements.

1.3 Purpose

The purpose of this document is to identify the procedures and instructions to operate and maintain Release A systems. In addition, DAAC staff responsibilities are identified. The DAAC M&O staff is comprised of operators, engineers, as well as operations support, administration and management staff personnel.

This document will also be used as a training aid for M&O staff who are located at the sites. The operations procedures and operations instructions were derived from, and are intended to be consistent with, the system functions and capabilities specified in the ECS design specifications and the operations activities described in the ECS Operations Concept Document.

1.4 Status and Schedule

This document is to be delivered at CSR minus two weeks. Updates will be made to reflect subsequent system releases. Changes will be submitted through established configuration management procedures, such as document change notices or published revisions.

1.5 Organization

The contents subsequent to this first section are presented as follows:

- Section 2. **Related Documentation.** Lists documents that drive, support or expand on the material in this manual.
- Section 3 **System Administration.** Identifies the operations procedures and/or operations instructions for system administration activities, such as backup and restore, log maintenance, user account administration, workstation installation,
- Section 4 **Database Administration.** Identifies the operations procedures and/or operations instructions for database administration activities, such as product installation, disk storage management, login and privileges administration, database validation, backup and recovery, database configuration, tuning and performance monitoring.
- Section 5 **Security Services.** Identifies the operations procedures and/or operations instructions for security services activities, such as user authentication and authorization, data access control, network services monitoring, password protection, file modification monitoring.
- Section 6 **Network Administration.** Identifies the operations procedures and/or operations instructions for network administration activities, such as network and system configuration monitoring, network services monitoring.
- Section 7 **System Monitoring.** Identifies the operations procedures and/or operations instructions for network system monitoring, such as problem monitoring and resolution.
- Section 8 **Problem Management.** Identifies the operations procedures and/or operations instructions for submitting trouble tickets and for processing and resolving trouble ticket submissions.
- Section 9 **Configuration Management.** Identifies the operations procedures and/or operations instructions for configuration management activities, such as CCB support, configuration item identification, configuration change requests (CCRs) submission and processing, configuration status accounting, configuration audits, data management, operational database maintenance, software transfer and installation.
- Section 10 **Metadata Administration.** Identifies the operations procedures and/or operations instructions for metadata administration activities, such as establishing collections, populating the database, specifying Earth Science Data Type (ESDT) services.

- Section 11 **Science Software Integration & Test (SSI&T) Operational Procedures.** Identifies the operations procedures and/or operations instructions to support SSI&T activities.
- Section 12 **Resource Planning.** Identifies the operations procedures and/or operations instructions for resource planning activities for non-routine ground events.
- Section 13 **Production Planning.** Identifies the operations procedures and/or operations instructions for production planning activities for job and resource prioritization and scheduling.
- Section 14 **Production Processing.** Identifies the operations procedures and/or operations instructions to support data processing activities.
- Section 15 **Quality Assurance.** Identifies the operations procedures and/or operations instructions to perform DAAC manual non-science quality assurance activities, such as visualization of science data products and updating quality assurance metadata.
- Section 16 **Ingest.** Identifies the operations procedures and/or operations instructions to support data acquisition.
- Section 17 **Archive.** Identifies the operations procedures and/or operations instructions for archiving activities, such as archive repository maintenance, fault monitoring and notification, temporary data storage.
- Section 18 **Data Distribution.** Identifies the operations procedures and/or operations instructions to support data distribution activities, such as media operations and product shipment.
- Section 19 **User Services.** Identifies the operations procedures and/or operations instructions to support user services activities to address user requests.
- Section 20 **Library Administration.** Identifies the operations procedures and/or operations instructions to support librarian administration activities, such as database administration of the Document Data Server Subsystem, change package preparation and distribution, master document control and maintenance.
- Section 21 **COTS Hardware Maintenance.** Identifies the operations procedures and/or operations instructions for preventive and corrective maintenance activities of COTS hardware for the ECS project.
- Section 22 **Software Maintenance.** Identifies the operations procedures and/or operations instructions to support maintenance activities for both COTS software, custom software, and science software.

- Section 23 **Property Management.** Identifies the operations procedures and/or operations instructions for the receipt, control, and accountability of ECS property at ECS sites during Release A.
- Section 24 **Installation Planning.** Identifies the operations procedures and/or operations instructions to support installation planning activities for conducting site surveys, ensuring that site preparations/coordination are completed on schedule, facilitating receipt and installation of the hardware.
- Section 25 **COTS Training.** Identifies the operations procedures and/or operations instructions to support COTS training activities, such as training request processing, training coordination, training scheduling, training record maintenance.
- Section 26 **On-line Advertising Service Administration.** Identifies the operations procedures and/or operations instructions for the Earth Science On-line Directory (ESOD) on-line advertising service activities, such as group administration and request processing.
- Appendix A **Miscellany.** Contains additional information related to previous sections.
- **Abbreviations and Acronyms.** Identifies abbreviations and acronyms used throughout this document.

2. Related Documentation

2.1 Parent Documents

The parent documents are the documents from which this Mission Operation Procedures' scope and content are derived.

423-41-01	Goddard Space Flight Center, EOSDIS Core System (ECS) Statement of Work
423-41-03	Goddard Space Flight Center, EOSDIS Core System (ECS) Contract Data Requirements Document

2.2 Applicable Documents

The following documents are referenced within this Mission Operation Procedures, or are directly applicable, or contain policies or other directive matters that are binding upon the content of this volume.

209-CD-001-003	Interface Control Document Between EOSDIS Core System (ECS) and the NASA Science Internet
209-CD-002-003	Interface Control Document Between EOSDIS Core System (ECS) and ASTER Ground Data System
209-CD-006-005	Interface Control Document Between the EOSDIS Core System (ECS) and the National Oceanic and Atmospheric Administration (NOAA) Affiliated Data Center (ADC) for the ECS Project
209-CD-007-004	Interface Control Document Between the EOSDIS Core System (ECS) and TRMM Science Data and Information System (TSDIS) for the ECS Project
209-CD-008-006	Interface Control Document Between the EOSDIS Core System (ECS) and the Goddard Space Flight Center (GSFC) Distributed Active Archive Center (DAAC) for the ECS Project
209-CD-009-002	Interface Control Document Between the EOSDIS Core System (ECS) and the Marshall Space Flight Center (MSFC) Distributed Active Archive Center (DAAC) for the ECS Project, Final
209-CD-010-005	Interface Control Document Between the EOSDIS Core System (ECS) and the Langley Research Center (LaRC) Distributed Active Archive Center (DAAC) for the ECS Project
209-CD-013-004	Interface Control Document Between the EOSDIS Core System (ECS) and the Landsat 7 System [for the ECS Project]
305-CD-002-002	Science Data Processing Segment (SDPS) Design Specification for the ECS Project

305-CD-003-002	Communications and System Management (CSMS) Design Specification for the ECS Project, Preliminary
305-CD-004-001	Overview of Release A SDPS and CSMS System Design Specification for the ECS Project
305-CD-005-001	Release A SDPS Client Subsystem Design Specification for the ECS Project
305-CD-006-001	Release A SDPS Interoperability Subsystem Design Specification for the ECS Project
305-CD-007-001	Release A SDPS Data Management Subsystem Design Specification for the ECS Project
305-CD-008-001	Release A SDPS Data Server Subsystem Design Specification for the ECS Project
305-CD-009-001	Release A SDPS Ingest Subsystem Design Specification [for the ECS Project]
305-CD-010-001	Release A SDPS Planning Subsystem Design Specification for the ECS Project
305-CD-011-001	Release A SDPS Data Processing Subsystem Design Specification for the ECS Project
305-CD-012-001	Release A CSMS Communications Subsystem Design Specification for the ECS Project
305-CD-013-001	Release A CSMS Systems Management Subsystem Design Specification for the ECS Project, Final
305-CD-014-001	Release A GSFC DAAC Design Specification for the ECS Project
305-CD-015-001	Release A LaRC DAAC Design Specification for the ECS Project
305-CD-016-001	Release A MSFC DAAC Design Specification for the ECS Project
305-CD-017-001	Release A EDC DAAC Design Specification for the ECS Project
305-CD-019-001	Release A System Monitoring and Coordination Center Design Specification for the ECS Project
305-CD-040-001	Flight Operations Segment (FOS) Design Specification for the ECS Project (Segment Level Design) Overview
305-CD-041-001	Flight Operations Segment (FOS) Planning and Scheduling Design Specification for the ECS Project
305-CD-042-001	Flight Operations Segment (FOS) Command Management Design Specification for the ECS Project
305-CD-043-001	Flight Operations Segment (FOS) Resource Management Design Specification for the ECS Project
305-CD-044-001	Flight Operations Segment (FOS) Telemetry Design Specification for the ECS Project
305-CD-045-001	Flight Operations Segment (FOS) Command Design Specification for the ECS Project

305-CD-046-001	Flight Operations Segment (FOS) Real-Time Contact Management Design Specification for the ECS Project
305-CD-047-001	Flight Operations Segment (FOS) Analysis Design Specification for the ECS Project
305-CD-048-001	Flight Operations Segment (FOS) User Interface Design Specification for the ECS Project
305-CD-049-001	Flight Operations Segment (FOS) Data Management Design Specification for the ECS Project
305-CD-050-001	Flight Operations Segment (FOS) Planning and Scheduling Program Design Language (PDL) for the ECS Project
305-CD-051-001	Flight Operations Segment (FOS) Command Management Program Design Language (PDL) for the ECS Project
305-CD-052-001	Flight Operations Segment (FOS) Resource Management Program Design Language (PDL) for the ECS Project
305-CD-053-001	Flight Operations Segment (FOS) Telemetry Program Design Language (PDL) for the ECS Project
305-CD-054-001	Flight Operations Segment (FOS) Real-Time Contact Management Program Design Language (PDL) for the ECS Project
305-CD-055-001	Flight Operations Segment (FOS) Analysis Program Design Language (PDL) for the ECS Project
305-CD-056-001	Flight Operations Segment (FOS) User Interface Program Design Language (PDL) for the ECS Project
305-CD-057-001	Flight Operations Segment (FOS) Data Management Program Design Language (PDL) for the ECS Project
305-CD-058-001	Flight Operations Segment (FOS) Command Program Design Language (PDL) for the ECS Project
313-CD-001-002	EOSDIS Core System (ECS) Internal Interface Control Document for the Flight Operations Segment
313-CD-004-001	Release A CSMS/SDPS Internal Interface Control Document for the ECS Project, Final
601-CD-001-004	Maintenance and Operations Management Plan for the ECS Project, Final
604-CD-001-004	Operations Concept for the ECS Project: Part 1-- ECS Overview
604-CD-003-002	Operations Concept for the ECS Project: Part 2A -- ECS Release A
605-CD-001-003	Operations Scenarios for the ECS Project: ECS Release A
609-CD-002-001	Release A Operations Tools Manual for the ECS Project
505-41-33	Goddard Space Flight Center, Interface Control Document Between EOSDIS Core System (ECS) and Science Computing Facilities (SCF), 1/96

2.3 Information Documents

2.3.1 Information Documents Referenced

The following documents are referenced herein and, amplify or clarify the information presented in this document. These documents are not binding on the content of the ECS Mission Operation Procedures for the ECS Project.

501-CD-001-004	Performance Assurance Implementation Plan (PAIP) for the ECS Project
532-CD-001-001	Release A Environmental Control Plan for the ECS Project
194-602-OP1-001	Property Management Plan for the ECS Project
613-CD-002-001	Release A COTS Maintenance Plan for the ECS Project
616-CD-001-002	Release A Integrated Logistics Support Plan for the ECS Project
622-CD-001-003	Training Plan for the ECS Project, Revision 2
423-41-02	Goddard Space Flight Center, Functional and Performance Requirements Specifications for the EOSDIS Core System (ECS)

2.3.2 Information Documents Not Referenced

The following documents, although not referenced herein and/or not directly applicable, do amplify or clarify the information presented in this document. These documents are not binding on the content of the Mission Operation Procedures for the ECS Project.

607-CD-001-002	ECS Maintenance and Operations Positions Descriptions for the ECS Project
----------------	---------------------------------------------------------------------------

3. System Administration

3.1 System Startup and Shutdown

The Startup and Shutdown processes begin when the System Administrator (SA) determines that it is necessary, determines the least impacting way to perform the startup or shutdown and appropriately notifies the people effected. When determining the least impacting way to perform the startup or shutdown, the SA takes into consideration if only certain server software packages need to be started/stopped or a whole system startup/shutdown is required. The SA also uses the information in this section's procedures to determine which other software/systems are dependent upon the one in consideration. Once these steps have been taken, the shutdown or startup is performed.

The Activity Checklist table that follows provides an overview of the startup and shutdown processes. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 3.1-1. Startup/Shutdown - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Determine that Startup/Shutdown is necessary.	(I) 3.1	
2	SA	Determine the Least Impacting Way to Perform the Startup/Shutdown.	(I) 3.1	
3	SA	Notify Those Effected by the Startup/Shutdown.	(I) 3.1	
4	SA	Perform the Startup/Shutdown	(P) 3.1	

3.1.1 Startup

3.1.1.1 Cold - By Subsystem

The System Startup process begins after a shutdown by the System Administrator (SA). The System Startup is done in sequential order by subsystem. This startup sequence is predetermined by the Network Administrator.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the SA has been properly trained to startup all aspects of the system and that the system is currently powered off (due to a normal or emergency shutdown).

Table 3.1-2 presents the steps required to perform a cold system startup. If you are already familiar with the procedures, you may prefer to use the quick-step tables. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

This section explains how to perform a cold system startup by subsystem. To begin a cold system startup, execute the procedure steps that follow:

1 Determine which machines perform the following functions:

- DNS Master
- NIS Master
- Mail Hub Server(s)
- Automount Servers
- Clearcase Server
- CSS:
 - DCE Server
 - DCE License Server for SUN
 - Other License Servers
- MSS:
 - Tivoli Server
 - Sybase SQL Servers
- DSS
- Ingest
- PDPS
- CIDM

- 2** Power on the DNS Master. Once the system has booted without error, proceed to step 3.
 - Remember to power on peripherals before powering on the CPU.
- 3** Power on the NIS Master. Once the system has booted without error, proceed to step 4.
 - Remember to power on peripherals before powering on the CPU.
- 4** Power on the Mail Hub server(s). Once the system(s) have booted without error, proceed to step 5.
 - Remember to power on peripherals before powering on the CPU.
- 5** Power on the Automount/Mail HUB server(s). Once the system(s) have booted without error, proceed to step 6.
 - Remember to power on peripherals before powering on the CPU.
- 6** Power on the Clearcase server(s). Once the systems(s) have booted without error, proceed to step 7.
 - Remember to power on peripherals before powering on the CPU.
- 7** Power on the CSS server(s). Once the system(s) have booted without error, proceed to step 8.
 - Remember to power on peripherals before powering on the CPU.

- 8** Power on the DCE License server for SUN. Once the system has booted without error, proceed to step 9.
 _ Remember to power on peripherals before powering on the CPU.
- 9** Power on the Other License server(s). Once the system(s) have booted without error, proceed to step 10.
 _ Remember to power on peripherals before powering on the CPU.
- 10** Power on the MSS server(s). Once the system(s) have booted without error, proceed to step 11.
 _ Remember to power on peripherals before powering on the CPU.
- 11** Power on the DSS server(s). Once the system(s) have booted without error, proceed to step 12.
 _ Remember to power on peripherals before powering on the CPU.
- 12** Power on the Ingest server(s). Once the system(s) have booted without error, proceed to step 13.
 _ Remember to power on peripherals before powering on the CPU.
- 13** Power on the PDPS server(s). Once the system(s) have booted without error, proceed to step 14.
 _ Remember to power on peripherals before powering on the CPU.
- 14** Power on the CIDM server(s).
 _ Remember to power on peripherals before powering on the CPU.

Table 3.1-2. Cold System Startup - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	determine subsystems
2	(No entry)	power on DNS Master
3	(No entry)	power on NIS Master
4	(No entry)	power on Mail Hub server(s)
5	(No entry)	power on Automount server(s)
6	(No entry)	power on Clearcase server(s)
7	(No entry)	power on CSS server(s)
8	(No entry)	power on DCE License server for SUN
9	(No entry)	power on Other License server(s)
10	(No entry)	power on MSS server(s)
11	(No entry)	power on DSS server(s)
12	(No entry)	power on Ingest server(s)
13	(No entry)	power on PDPS server(s)
14	(No entry)	power on CIDM server(s)

3.1.1.2 Warm - By Server Software

The System Startup by Server Software process is performed by the System Administrator (SA). The system startup is normally performed in reverse order of the system shutdown.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the Startup has been scheduled well in advance, all planning involved has been concluded well in advance and the SA has been properly trained to startup all aspects of the system.

Table 3.1-3 presents the steps required to perform a normal system startup. If you are already familiar with the procedures, you may prefer to use the quick-step tables. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

The order of this Startup is contingent on software dependencies. Please refer to Section 4.2.2.7 of the ECS Operations Concept procedures (604-CD-002-003) for further instructions.

Table 3.1-3. Warm System Startup - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	determine software dependencies
2	(No entry)	reboot independent server(s)
3	(No entry)	reboot dependent server(s)

3.1.2 Shutdown

3.1.2.1 Normal - By Subsystem

The Normal System Shutdown process is performed at the discretion of the System Administrator (SA), usually for the purpose of repair. The system shutdown is **normally performed in reverse order of the system startup.**

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the Shutdown has been scheduled well in advance, all planning involved has been concluded well in advance and the SA has been properly trained to shutdown all aspects of the system.

Table 3.1-4 presents the steps required to perform a normal system shutdown. If you are already familiar with the procedures, you may prefer to use the quick-step tables. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

This section explains how to perform a normal system shutdown by subsystem.

3.1.2.1.1 Shutdown a Machine

The SA must be logged in as root to perform a shutdown. To begin a normal system shutdown, execute the procedure steps that follow:

- 1 Login to the server as root.
- 2 Enter root password.
- 3 Type **wall** and press **Return**.
- 4 Type **This machine is being shutdown for reason. Please save your work and log off now. We are sorry for the inconvenience.** Press Control and D keys simultaneously.
- 5 Wait at least five minutes.
- 6 Type **shutdown -g600 -i0** UNIX prompt and press **Return**.
- 7 Power off all peripherals and the CPU.

The servers should be shutdown in the following order:

- 1 Determine which machines perform the following functions:
 - DNS Master
 - NIS Master
 - Mail Hub Server(s)
 - Automount Server
 - Clearcase Server
 - CSS:
 - DCE Server
 - DCE License Server for SUN
 - Other License Servers
 - MSS:
 - Tivoli Server
 - Sybase SQL Servers
 - DSS
 - Ingest
 - PDPS
 - CIDM
- 2 Shutdown the CIDM server(s) by following procedure 3.1.2.1.1 for each machine. Once the system(s) have shutdown without error, proceed to step 3.
- 3 Shutdown the PDPS server(s) by following procedure 3.1.2.1.1 for each machine. Once the system(s) have shutdown without error, proceed to step 4.
- 4 Shutdown the Ingest server(s) by following procedure 3.1.2.1.1 for each machine. Once the system(s) have shutdown without error, proceed to step 5.

- 5 Shutdown the DSS server(s) by following procedure 3.1.2.1.1 for each machine. Once the system(s) have shutdown without error, proceed to step 6.
- 6 Shutdown the MSS server(s) by following procedure 3.1.2.1.1 for each machine. Once the system(s) have shutdown without error, proceed to step 7.
- 7 Shutdown the Other License server(s) by following procedure 3.1.2.1.1 for each machine. Once the system(s) have shutdown without error, proceed to step 8.
- 8 Shutdown the DCE License server for the SUN by following procedure 3.1.2.1.1 for each machine. Once the system(s) have shutdown without error, proceed to step 9.
- 9 Shutdown the CSS server(s) by following procedure 3.1.2.1.1 for each machine. Once the system(s) have shutdown without error, proceed to step 10.
- 10 Shutdown the Clearcase server(s) by following procedure 3.1.2.1.1 for each machine. Once the system(s) have shutdown without error, proceed to step 11.
- 11 Shutdown the Automount server(s) by following procedure 3.1.2.1.1 for each machine. Once the system(s) have shutdown without error, proceed to step 12.
- 12 Shutdown the Mail Hub server(s) by following procedure 3.1.2.1.1 for each machine. Once the system(s) have shutdown without error, proceed to step 13.
- 13 Shutdown the NIS Master by following procedure 3.1.2.1.1 for each machine. Once the system has shutdown without error, proceed to step 14.
- 14 Shutdown the DNS Master by following procedure 3.1.2.1.1 for each machine.

Table 3.1-4. Normal System Shutdown - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	determine subsystems and server dependencies
2	(No entry)	Login to the server as root
3	wall	Press Return
4	This machine is being shutdown for <i>reason</i> . Please save your work and log off now. We are sorry for the inconvenience.	Press Control and D keys simultaneously
5	(No entry)	Wait at least five minutes
6	shutdown -g0 -i0 or shutdown now -i0	Press Return
7	(No entry)	Power off all peripherals and the CPU.
8	(No entry)	Repeat steps 2 through 7 above for all servers

3.1.2.2 Emergency - By Subsystem

The Emergency System Shutdown process begins after it is determined that the system may fail during emergency situations (i.e., storms, power outages) by the System Administrator (SA). The Emergency System Shutdown is done in sequential order by subsystem. This shutdown sequence is predetermined by the Network Administrator.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the SA has been properly trained to shutdown all aspects of the system.

Table 3.1-5 presents the steps required to perform a Emergency System Shutdown. If you are already familiar with the procedures, you may prefer to use the quick-step tables. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

This section explains how to perform an emergency system shutdown by subsystem. The SA must be logged in as root to perform a shutdown. To begin an emergency system shutdown, execute the procedure steps that follow:

- 1 Login to the server as root.
- 2 Enter root password.
- 3 Type **sync** at the UNIX prompt and hit **Return**.

Sync executes the sync system primitive. If the system is to be stopped, sync must be called to insure file system integrity. It will flush all previously unwritten system buffers out to disk, thus assuring that all file modifications up to that point will be saved.
- 4 Type **sync** again at the UNIX prompt and hit **Return**.
- 5 Type **halt** at the UNIX prompt and hit **Return**.
- 6 Once the halt has completed, turn the power switch on the CPU and all peripherals to off.

The servers should be shutdown in the following order:

- 1 Shutdown all client workstations.
- 2 Determine which machines perform the following functions:

Sybase SQL/Rep
Autosys
Clearcase
Tivoli
DCE
Automount

Mail Hub
NIS
DNS

- 3** Shutdown the Sybase SQL/Rep server(s). Once the system has shutdown without error, proceed to step 4.
- 4** Shutdown the Autosys server(s). Once the system has shutdown without error, proceed to step 5.
- 5** Shutdown the Clearcase server(s). Once the system has shutdown without error, proceed to step 6.
- 6** Shutdown the Tivoli server(s). Once the system has shutdown without error, proceed to step 7.
- 7** Shutdown the DCE server(s). Once the system has shutdown without error, proceed to step 8.
- 8** Shutdown the Automount server(s). Once the system has shutdown without error, proceed to step 9.
- 9** Shutdown the Mail Hub server(s). Once the sytem has shutdown without error, proceed to step 10.
- 10** Shutdown the NIS server(s). Once the system has shutdown without error, proceed to step 11.
- 11** Shutdown the DNS server(s).

In case of EXTREME emergency where time does not allow you to execute the above procedures, execute the following procedure steps for Sun machines:

- 1** Login to the server as root.
- 2** Enter root password.
- 3** Hit the L1 or Stop key and the “a” key simultaneously.
- 4** Once returned to an ok or > prompt, turn the power switches on the CPU and all peripherals to off.

NOTE: The use of L1a does not ensure file system integrity. There is a very high risk of losing data when using this process.

Table 3.1-5. Emergency System Shutdown - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	determine subsystems and server dependencies
2	(No entry)	Login to server as root
3	(No entry)	Type sync at prompt and press enter
4	(No entry)	Type sync at prompt and press enter
5	(No entry)	Type halt at prompt and press enter
6	(No entry)	Turn power switches on CPU and all peripherals to off.
7	(No entry)	Repeat steps 2 through 5 above for all servers

3.1.2.3 Server - By Server Software

The System Shutdown by Server Software process is performed by the System Administrator (SA). The system shutdown is normally performed in reverse order of the system startup.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the Shutdown has been scheduled well in advance, all planning involved has been concluded well in advance and the SA has been properly trained to shutdown all aspects of the system.

Table 3.1-6 presents the steps required to perform a normal system shutdown. If you are already familiar with the procedures, you may prefer to use the quick-step tables. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

The order of this Shutdown is contingent on software dependencies. Please refer to section 4.2.2.7 of the ECS Operations Concept procedures (604-CD-002-003) for further instructions.

Table 3.1-6. Server System Shutdown - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	determine software dependencies
2	(No entry)	shutdown dependent server(s)
3	(No entry)	shutdown independent server(s)

3.2 System Backup and Restore

3.2.1 Incremental Backup

Non-scheduled incremental backups can be requested at any time by submitting a Request for Incremental Backup form to the supervisor. The supervisor schedules the request with the SA who performs the incremental backup. Afterwards, the SA notifies the requester and supervisor that the incremental backup is complete.

The Activity Checklist table that follows provides an overview of the incremental backup process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 3.2-1. Incremental Backup - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request for Incremental Backup to Ops Supervisor.	(I) 3.2.1	
2	Ops Super	Schedule Incremental Backup with SA.	(I) 3.2.1	
3	SA	Perform Incremental Backup.	(P) 3.2.1	
4	SA	Notify Requester and Ops Super when Incremental Backup is Complete.	(I) 3.2.1	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for an incremental backup has already been approved by DAAC Management. In order to perform the procedure, the SA must have obtained the following information from the requester:

a. **Name of machine to be backed up**

Table 3.2-2 presents the steps required to perform an incremental backup in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To perform an incremental backup for the requester, execute the procedure steps that follow:

Note 1: If you run out of tapes at any time during this procedure, execute procedure 3.2.5.2 Labeling Tapes and then return to this procedure.

- 1 Log into the **machine to be backed up** by typing: **telnet *BackedUpSystemName*** or **rsh *BackedUpSystemName***, then press **Return**.
- 2 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.
 - _ A password prompt is displayed.
- 3 Enter ***YourPassword***, then press **Return**.
 - _ Remember that ***YourPassword*** is case sensitive.
 - _ You are authenticated as yourself and returned to the UNIX prompt.

- 4 Log in as root by typing: **su**, then press **Return**.
 - _ A password prompt is displayed.
- 5 Enter the **RootPassword**, then press **Return**.
 - _ Remember that the **RootPassword** is case sensitive.
 - _ You are authenticated as root and returned to the UNIX prompt.
- 6 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY BackupServerName:0.0**, then press **Return**.
- 7 Execute the NetWorker Administrative program by entering: **nwadmin**, then press **Return**.
 - _ A window opens for the NetWorker Administrative program.
 - _ You are now able to perform an incremental backup.
- 8 Go to the **Customize** menu, select **Schedules**.
 - _ The **Schedules** window opens.
- 9 Look at the button for today. If there is an **i** next to the date on this button, go to step 12.
 - _ The **i** stands for incremental. A **f** stands for full. Whichever is on the button for today is what kind of backup that will be done, unless it is overridden.
- 10 Click and hold the button for today, select **Overrides** from the resulting menu, select **Incremental** from the next resulting menu.
- 11 Click the **Apply** button.
- 12 Close the **Schedules** window by clicking in the upper left corner of the **Schedules** window and selecting **Close** from the resulting menu.
- 13 Click the **Group Control** button.
 - _ The **Group Control** window opens.
- 14 Click the **Start** button.
 - _ A **Notice** window opens.
- 15 Click the **OK** button.
 - _ The **Notice** window closes.
 - _ The regularly scheduled backup will still run (even though we are now doing a backup).
- 16 Close the **Group Control** window by clicking in the upper left corner of the **Group Control** window and selecting **Close** from the resulting menu.
 - _ Status updates appear in the **nwadmin** window.
 - _ When the backup is complete, a **Finished** message will appear.
- 17 If the button for today in step 9 had an **i** on it, go to step 22.

- 18 Go to the **Customize** menu, select **Schedules**.
 _ The **Schedules** window opens.
- 19 Click and hold the button for today, select **Overrides** from the resulting menu, select **Full** from the next resulting menu.
- 20 Click the **Apply** button.
- 21 Close the **Schedules** window by clicking in the upper left corner of the **Schedules** window and selecting **Close** from the resulting menu.
- 22 Select **Exit** from the **File** menu to quit the NetWorker Administrative program.
 _ The **nwadmin** window closes.
- 23 At the UNIX prompt for the **machine to be backed up**, type **exit**, then press **Return**.
 _ **Root** is logged out.
- 24 Type **exit** again, then press **Return**.
 _ You are logged out and disconnected from the **machine to be backed up**.

To perform an incremental backup, execute the steps provided in the following table.

Table 3.2-2. Perform Incremental Backup - Quick-Step Procedures (1 of 2)

Step	What to Enter or Select	Action to Take
1	telnet <i>BackedUpSystemName</i> -or- rsh <i>BackedUpSystemName</i>	press Return
2	<i>YourUserID</i> or- (No entry)	press Return -or- (No action)
3	<i>YourPassword</i>	press Return
4	su	press Return
5	<i>RootPassword</i>	press Return
6	setenv DISPLAY <i>IPNumber:0.0</i> -or- setenv DISPLAY <i>BackedUpSystemName:0.0</i>	press Return
7	nwadmin	press Return
8	Customize → Schedules	if i on today's button then go to step 10. Otherwise, click and hold today's button.
9	Overrides → Incremental	click Apply button
10	(No entry)	close Schedules window
11	(No entry)	click Group Control button
12	(No entry)	click Start button
13	(No entry)	click OK button
14	(No entry)	close Group Control window
15	(No entry)	if there was an i on today's button in step 8, go to step 18.

Table 3.2-2. Perform Incremental Backup - Quick-Step Procedures (2 of 2)

Step	What to Enter or Select	Action to Take
16	Customize → Schedules	click and hold today's button
17	Overrides → Full	click Apply button
18	(No entry)	close Schedules window
19	File → Exit	(No action)
20	exit	press Return
21	exit	press Return

3.2.2 Full Backup

Non-scheduled full backups can be requested at any time by submitting a Request for Full Backup form to the supervisor. The supervisor schedules the request with the SA who performs the full backup. Afterwards, the SA notifies the requester and supervisor that the full backup is complete.

The Activity Checklist table that follows provides an overview of the full backup process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 3.2-3. Full Backup - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request for Full Backup to Ops Supervisor.	(I) 3.2.2	
2	Ops Super	Schedule Full Backup with SA.	(I) 3.2.2	
3	SA	Perform Full Backup.	(P) 3.2.2	
4	SA	Notify Requester and Ops Super when Full Backup is Complete.	(I) 3.2.2	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for a full backup has already been approved by DAAC Management. In order to perform the procedure, the SA must have obtained the following information from the requester:

- a. **Name of machine to be backed up**

b. **Files/directories to be backed up** (optional)

Table 3.2-4 presents the steps required to perform a full backup in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To perform a full backup for the requester, execute the procedure steps that follow:

Note 1: If you run out of tapes at any time during this procedure, execute procedure 3.2.5.2 Labeling Tapes and then return to this procedure.

- 1 Log into the **machine to be backed up** by typing: **telnet *BackedUpSystemName*** or **rsh *BackedUpSystemName***, then press **Return**.
- 2 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.
 - _ A password prompt is displayed.
- 3 Enter ***YourPassword***, then press **Return**.
 - _ Remember that ***YourPassword*** is case sensitive.
 - _ You are authenticated as yourself and returned to the UNIX prompt.
- 4 Log in as root by typing: **su**, then press **Return**.
 - _ A password prompt is displayed.
- 5 Enter the ***RootPassword***, then press **Return**.
 - _ Remember that the ***RootPassword*** is case sensitive.
 - _ You are authenticated as root and returned to the UNIX prompt.
- 6 Set display to current terminal by typing: **setenv DISPLAY *IPNumber:0.0*** or **setenv DISPLAY *BackedUpSystemName:0.0***, then press **Return**.
- 7 Execute the NetWorker Backup program by entering: **nwbackup**, then press **Return**.
 - _ A **NetWorker Backup** window opens.
 - _ You are now able to perform a full backup.
- 8 If no **files/directories to be backed up** were provided, i.e. the whole machine is to be backed up, then type **/** in the **Selection** field and click the **Mark** button.
 - _ **/** is designated for backup and has a check next to it.
- 9 If **files/directories to be backed up** were provided then select the **files/directories to be backed up** in the directory display and click the **Mark** button.
 - _ Drag scroll bar with mouse to scroll the list up and down.
 - _ Double click on directory name to list its contents.
 - _ To move up a directory level, type the path in the **Selection** field.
 - _ Clicking the **Mark** button designates the file for backup and puts a check next to it.

- 10 Click the **Start** button.
 - _ A **Backup Options** window opens.
- 11 Click the **OK** button.
 - _ The **Backup Options** window closes.
 - _ The **Backup Status** window opens providing updates on the backup's progress.
- 12 After the **Backup Completion Time** message appears in the **Backup Status** window, click the **Cancel** button.
 - _ The **Backup Status** window closes.
 - _ The backup is complete.
- 13 Select **Exit** from the **File** menu to quit the NetWorker Backup program.
 - _ The **NetWorker Backup** window closes.
- 14 At the UNIX prompt for the **machine to be backed up**, type **exit**, then press **Return**.
 - _ **Root** is logged out.
- 15 Type **exit** again, then press **Return**.
 - _ You are logged out and disconnected from the **machine to be backed up**.

To perform a full backup, execute the steps provided in the following table.

Table 3.2-4. Perform Full Backup - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	telnet <i>BackedUpSystemName</i> -or- rsh <i>BackedUpSystemName</i>	press Return
2	<i>YourUserID</i> -or- (No entry)	press Return -or- (No action)
3	<i>YourPassword</i>	press Return
4	su	press Return
5	<i>RootPassword</i>	press Return
6	setenv DISPLAY <i>IPNumber:0.0</i> -or- setenv DISPLAY <i>BackedUpSystemName:0.0</i>	press Return
7	nwbackup	press Return
8	to back up whole machine , / in selection field	click Mark button
9	to back up certain files/directories , the files/directories	click Mark button
10	(No entry)	click Start button
11	(No entry)	click OK button
12	(No entry)	click Cancel button
13	File → Exit	(No action)
14	exit	press Return
15	exit	press Return

3.2.3 File Restore

The File Restore process begins when the requester submits a request to the SA. The SA restores the file(s) and notifies the requester when complete.

The Activity Checklist table that follows provides an overview of the file restore process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 3.2-5. File Restore - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request for File Restore to SA.	(I) 3.2.3	
2	SA	Restore file(s).	(P) 3.2.3	
3	SA	Inform Requester of completion.	(I) 3.2.3	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for a file restore has already been approved by the Supervisor. In order to perform the procedure, the SA must have obtained the following information from the requester:

- a. **Name of machine to be restored**
- b. **Name of file(s) to be restored**
- c. **Date from which to restore**
- d. **User ID of the owner of the file(s) to be restored**
- e. **Choice of action to take when conflicts occur. Choices are:**
 - **rename current file**
 - **keep current file**
 - **write over current file with recovered file**

Table 3.2-6 contains a table which presents the steps required to restore a file in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

To restore a file for the requester, execute the procedure steps that follow:

- 1 Log into the **machine to be restored** by typing: **telnet *MachineRestored*** or **rsh *MachineRestored***, then press **Return**.
- 2 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.
 - _ A password prompt is displayed.
- 3 Enter ***YourPassword***, then press **Return**.
 - _ Remember that ***YourPassword*** is case sensitive.
 - _ You are authenticated as yourself and returned to the UNIX prompt.
- 4 Log in as **root** by typing: **su**, then press **Return**.
 - _ A password prompt is displayed.
- 5 Enter the ***RootPassword***, then press **Return**.
 - _ Remember that the ***RootPassword*** is case sensitive.
 - _ You are authenticated as **root** and returned to the UNIX prompt.
- 6 Log in as the **user requesting restore** by typing: **su *User'sID***
 - _ You are authenticated as the **owner of the file(s) to be restored**.
- 7 Set display to current terminal by typing: **setenv DISPLAY *IPNumber:0.0*** or **setenv DISPLAY *MachineRestored:0.0***, then press **Return**.
- 8 Execute the **NetWorker Recovery** program by entering: **nwrecover**, then press **Return**.
 - _ A window opens for the **NetWorker Recovery** program.
 - _ You are now able to perform restores of files.
- 9 Select **file(s) to be restored** and click the **Mark** button.
 - _ Drag scroll bar with mouse to scroll the list up and down.
 - _ **Double click** on directory name to list its contents.
 - _ **Clicking** the **Mark** button designates the file for restore and puts a check next to it.
- 10 Go to the **Change** menu, select **Browse Time**.
 - _ The Change Browse Time window opens.
- 11 Select the **date from which to restore**.
 - _ **NetWorker** will automatically go to that day's or a previous day's backup which contains the file.
- 12 Click the **Start** button.
 - _ The Conflict Resolution window opens.

- 13 Answer “**Do you want to be consulted for conflicts**” by clicking the **yes** button, then click the **OK** button.
 - If prompted with a conflict, choices of action will be: **rename current file, keep current file, or write over current file with recovered file**. Select the requester’s **choice of action to take when conflicts occur**.
 - The **Recover Status** window opens providing information about the file restore.
 - If all the required tapes are not in the drive, a notice will appear. Click the **OK** button in the notice window.
 - If prompted for tapes, click cancel in the **Recover Status** window and execute procedure 3.2.5.1.1 Index Tapes.
- 14 When a recovery complete message appears, click the **Cancel** button.
- 15 Go to the **File** menu, select **Exit**.
 - The **NetWorker Recovery** program quits.
- 16 Type **exit**, then press **Return**.
 - The **owner of the file(s) to be restored** is logged out.
- 17 Type **exit** again, then press **Return**.
 - **Root** is logged out
- 18 Type **exit** one last time, then press **Return**.
 - You are logged out and disconnected from the **machine to be restored**.

To restore a file, execute the steps provided in the following table.

Table 3.2-6. Restore a File - Quick-Step Procedures (1 of 2)

Step	What to Enter or Select	Action to Take
1	telnet <i>MachineRestored</i> -or- rsh <i>MachineRestored</i>	press Return
2	<i>YourUserID</i> -or- (No entry)	press Return -or- (No action)
3	<i>YourPassword</i>	press Return
4	su	press Return
5	<i>RootPassword</i>	press Return
6	su <i>User'sID</i>	press Return
7	setenv DISPLAY <i>IPNumber:0.0</i> -or- setenv DISPLAY <i>MachineRestored:0.0</i>	press Return
8	nwrecover	press Return
9	file(s) to be restored	click the Mark button
10	Change → Browse Time	(No action)
11	date from which to restore	click the Start button
12	yes	click OK button

Table 3.2-6. Restore a File - Quick-Step Procedures (2 of 2)

Step	What to Enter or Select	Action to Take
14	(No entry)	choose what action to take when notified of conflicts
15	(No entry)	click Cancel button
16	File → Exit	(No action)
17	exit	press Return
18	exit	press Return
19	exit	press Return

3.2.4 Complete System Restore

The Complete System Restore process begins when the requester has determined that a complete system restore is the only way to resolve the problem and has approval from DAAC management. Once notified of the request, the SA performs restores of all partitions on the system. Afterwards, the SA documents and logs all actions in the operator's log book and notifies the requester and DAAC Manager that the complete system restore is complete.

The Activity Checklist table that follows provides an overview of the complete system restore process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 3.2-7. Complete System Restore - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Trouble Shoot and Determine that a Complete System Restore is necessary.	(I) 3.2.4	
2	SA	Restore all Partitions on the System	(P) 3.2.4	
3	SA	Document and Log in operator's log book, and Inform Requester and DAAC Manager of completion.	(I) 3.2.4	

Detailed procedures for tasks performed by the SA are provided in the sections that follow. The procedures assume that the requester's application for a complete system restore has already been approved by DAAC Management. In order to perform the procedure, the SA must have obtained the following information about the requester:

- a. **Name of system to be restored**
- b. **Date from which to restore**

A complete system restore involves restoring all partitions on that system.

Table 3.2-8 presents the steps required to restore a partition in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To restore a partition for the requester, execute the procedure steps that follow:

- 1 Log into the backup server by typing: **telnet *BackupServerName*** or **rsh *BackupServerName***, then press **Return**.
- 2 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.
 - _ A password prompt is displayed.
- 3 Enter ***YourPassword***, then press **Return**.
 - _ Remember that ***YourPassword*** is case sensitive.
 - _ You are authenticated as yourself and returned to the UNIX prompt.
- 4 Log in as **root** by typing: **su**, then press **Return**.
 - _ A password prompt is displayed.
- 5 Enter the ***RootPassword***, then press **Return**.
 - _ Remember that the ***RootPassword*** is case sensitive.
 - _ You are authenticated as **root** and returned the UNIX prompt.
- 6 Set display to current terminal by typing: **setenv DISPLAY *IPNumber:0.0*** or **setenv DISPLAY *BackupServerName:0.0***, then press **Return**.
- 7 Execute the **NetWorker Administrator** program by entering: **nwadmin**, then press **Return**.
 - _ A window opens for the **NetWorker Administrator** program.
 - _ You are now able to perform restores of partitions.
- 8 Go to the **Save Set** menu, select **Recover Set**.
 - _ The **Save Set Recover** window opens.
- 9 Select the **Name of system to be restored** (referred to as **System** in the rest of this procedure) in the **Client** field's menu.
 - _ The **Save Set** listing updates. This is a listing of partitions on the **System**.
 - _ At this time, note the partitions listed for the **System**. To do a complete system restore, this procedure needs to be performed for each partition listed.
- 10 Select the **Save Set/partition** from the listing.
 - _ The **Instance** listing updates.
- 11 Select the appropriate **Instance**.

- An **Instance** is a particular **NetWorker** client backup. A listing of **Instances** is a report detailing the **NetWorker** client backups that have occurred.
- Select an **Instance** based upon the **Date from which to restore** (referred to as **Date** in the rest of this procedure) and of an appropriate level:

Note 1: To determine a base **Date**, you must consider the time of day that backups occur. For example, if the backup occurs at 02:00 each morning then a system corrupted at noon on June 6 would require a restoration of the June 6 backup. However, if the system corruption took place around the time of the backup, it would be more prudent to use the backup from June 5.

- If the backups are full or incremental, perform the following actions:
Select the most recent full backup that occurred on or prior to the **Date** and perform a partition restore. If the date of this full backup is not the same as the **Date**, perform a partition restore using each incremental backup, in chronological order, between this full backup and the day after the **Date**.
- If the backups are of different numerical levels, follow these steps:
First select the most recent level 0/full backup prior to or on the **Date** and perform a restore of the partition. If a level 0/full backup did not occur on the **Date**, select the most recent backup of the next highest level occurring after this level 0 and prior to or on the **Date**. Perform a restore of the partition. Continue to select the most recent backup of the next highest level occurring between the last used **Instance** and the day after the **Date** until reaching an instance on the **Date**.

- You can double click an **Instance** to see which tape is required.

12 Click the **Recover** button.

- The **Save Set Recover Status** window opens.
- Clicking the **Volumes** button will show which tapes are required.

13 Click the **Options** button.

- The Save Set Recover Options window opens.

14 Set **Duplicate file resolution** to **Overwrite existing file** by clicking its radio button.

15 Make sure that the **Always prompt** checkbox is not checked.

16 Click the **OK** button.

- The Save Set Recover Options window closes.

17 Click the **Start** button in the **Save Set Recover Status** window.

- Status messages appear in the **Status** box.
- If prompted for tapes, click the **Cancel** button in the **Save Set Recover Status** window and follow steps 8-14 of procedure 3.2.5.1.1 Index Tapes (or steps 8-15 of procedure 3.2.5.1.2 Index Tapes Quick Steps)
- A **recovery complete** message appears when recovery is complete.

- 18 Click the **Cancel** button after the **recovery complete** message appears.
_ The Save Set Recover Status window closes.
- 19 If additional partition restores are required, go to step 8. Otherwise, select **Exit** from the **File** menu to quit the NetWorker Administrator program.
- 20 At the UNIX prompt for the backup server, type **exit**, then press **Return**.
- 21 Type **exit** again, then press **Return**.

To restore a partition, execute the steps provided in the following table.

Table 3.2-8. Restore a Partition - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	telnet <i>BackupServerName</i> -or- rsh <i>BackupServerName</i>	press Return
2	<i>YourUserID</i>	press Return
3	<i>YourPassword</i>	press Return
4	su	press Return
5	<i>RootPassword</i>	press Return
6	setenv DISPLAY <i>IPNumber.0.0</i> -or- setenv DISPLAY <i>BackupServerName:0.0</i>	press Return
7	nwadmin	press Return
8	Save Set → Recover Set	(no action)
9	Client/System	(no action)
10	Save Set/partition	(no action)
11	Instance	click Recover button
12	(No entry)	click Options button
13	Overwrite existing file	deselect Always prompt
14	(No entry)	click OK button
15	(No entry)	click Start button
16	(No entry)	click Cancel button
17	(No entry)	go to step 8 -or- select File → Exit
18	exit	press Return
19	exit	press Return

3.2.5 Tape Handling

3.2.5.1 Indexing Tapes

The Indexing Tapes process begins when the SA is performing procedures 3.2.3 File Restore or 3.2.4 Complete System Restore (or their associated Quick Steps) and is notified that the required tape(s) is/are not in the jukebox. The tape(s) must be pulled from tape storage, installed in the jukebox and indexed. If the tape(s) is/are not indexed, Networker will not be aware of it/them. After indexing the required tape(s), the SA resumes procedure 3.2.3 or 3.2.4.

The Activity Checklist table that follows provides an overview of the indexing tapes process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 3.2-9. Indexing Tapes - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Pull Required Tape(s) from Tape Storage.	(I) 3.2.5.1	
2	SA	Index Tapes	(P) 3.2.5.1	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the SA was previously executing procedure 3.2.3 or 3.2.4. In order to perform the procedure, the SA must have obtained the following:

a. **The required tape(s)**

Table 3.2-10 presents the steps required to index tapes in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To index tapes, execute the procedure steps that follow:

- 1 Log into the **backup server** by typing: **telnet BackupServerName** or **rsh BackupServerName** at the UNIX prompt, then press **Return**.
- 2 If a **Login:** prompt appears, log in as yourself by typing: **YourUserID**, then press **Return**.
_ A password prompt is displayed.

- 3 Enter ***YourPassword***, then press **Return**.
 - _ Remember that ***YourPassword*** is case sensitive.
 - _ You are authenticated as yourself and returned to the UNIX prompt.
- 4 Log in as **root** by typing: **su**, then press **Return**.
 - _ A password prompt is displayed.
- 5 Enter the ***RootPassword***, then press **Return**.
 - _ Remember that the ***RootPassword*** is case sensitive.
 - _ You are authenticated as **root** and returned the UNIX prompt.
- 6 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY BackupServerName:0.0**, then press **Return**.
- 7 Execute the **Networker Administrative** program by entering: **nwadmin**, then press **Return**.
 - _ A window opens for the **Networker Administrative** program.
 - _ You are now able to index tapes.
 - _ Click the **Mount** button to show what tapes **Networker** is currently aware of. The **Jukebox Mounting** window opens. Once finished with this window, click the **Cancel** button.
- 8 Put the **required tape(s)** in the jukebox's cartridge, install the cartridge in the jukebox.
 - _ For instructions, refer to the jukebox's documentation.
- 9 Go to the **Media** menu, select **Inventory**.
 - _ The **Jukebox Inventory** window opens.
- 10 Enter **2** in the **First Slot** field, enter **11** in the **Last Slot** field.
 - _ **Slot 1** is the non-removable slot within the jukebox. This usually contains a cleaning tape or a tape that is used on a regular basis.
 - _ **Slot 2** is at the top of the cartridge and **11** at the bottom.
 - _ It is OK to have empty slots or slots with tapes which have already been indexed.
- 11 Click the **OK** button.
 - _ A checking volume message appears and updates.
 - _ Performing an inventory on a full cartridge takes about twenty minutes.
- 12 When the status in the **Jukebox Inventory** window says finished, click the **Cancel** button.
 - _ The **Jukebox Inventory** window closes.
- 13 Click the **Mount** button to verify that the indexing worked.
 - _ The **Jukebox Mounting** window opens.
 - _ The **required tape(s)** should be shown. If not, repeat this procedure from step 8.

- 14 Click the **Cancel** button.
_ The **Jukebox Mounting** window closes.
- 15 Go to the **File** menu, select **Exit**.
- 16 At the UNIX prompt for the *backupserver*, type **exit**, then press **Return**.
- 17 Type **exit** again, then press **Return**.
- 18 Resume procedure 3.2.3 at step 12, procedure 3.2.3 at quick-step 11 - action part, procedure 3.2.4 at step 12, or procedure 3.2.4 at quick-step 11 - action part.

To index tapes, execute the steps provided in the table.

Table 3.2-10. Index Tapes - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	telnet <i>BackupServerName</i> -or- rsh <i>BackupServerName</i>	press Return
2	<i>YourUserID</i> -or- (No entry)	press Return -or- (No action)
3	<i>YourPassword</i>	press Return
4	su	press Return
5	<i>RootPassword</i>	press Return
6	setenv DISPLAY <i>IPNumber:0.0</i> -or- setenv DISPLAY <i>BackupServerName:0.0</i>	press Return
7	nwadmin	press Return
8	(No entry)	put required tape(s) in cartridge and install cartridge in jukebox
9	Media → Inventory	(No action)
10	2	(No action)
11	11	click OK button
12	(No entry)	click Cancel button
13	(No entry)	click Mount button
14	(No entry)	verify indexing
15	(No entry)	click Cancel button
16	File → Exit	(No action)
17	exit	press Return
18	exit	press Return
19	(No entry)	resume previous procedure

3.2.5.2 Labeling Tapes

The Labeling Tapes process begins when the SA is performing procedures 3.2.1 Incremental Backup or 3.2.2 Full Backup (or their associated Quick Steps) and runs out of tapes. The tape(s) must be installed in the jukebox and labeled. NetWorker uses tape labels for identification. The label that NetWorker creates is on the tape media itself, rather than a sticker on the outside of the tape cassette. An index is kept by NetWorker associating tape labels with particular backups/data. When you select files to recover using the NetWorker Recover window or view saved sets on a backup volume using the Volume Management window in NetWorker, you are viewing this index. After labeling the required tape(s), the SA resumes procedure 3.2.1 or 3.2.2.

The Activity Checklist table that follows provides an overview of the labeling tapes process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 3.2-11. Labeling Tapes - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Install Required Tape(s) in Jukebox	(I) 3.2.5.2	
2	SA	Label Tapes	(P) 3.2.5.2	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the SA was previously executing procedure 3.2.1 or 3.2.2. In order to perform the procedure, the SA must have obtained the following:

a. **Blank tape(s)**

Table 3.2-12 presents the steps required to label tapes in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To label tapes, execute the procedure steps that follow:

- 1 Log into the **backup server** by typing: **telnet BackupServerName** or **rsh BackupServerName** at the UNIX prompt, then press **Return**.
- 2 If a **Login:** prompt appears, log in as yourself by typing: **YourUserID**, then press **Return**.
_ A password prompt is displayed.

- 3 Enter ***YourPassword***, then press **Return**.
 - _ Remember that ***YourPassword*** is case sensitive.
 - _ You are authenticated as yourself and returned to the UNIX prompt.
- 4 Log in as **root** by typing: **su**, then press **Return**.
 - _ A password prompt is displayed.
- 5 Enter the ***RootPassword***, then press **Return**.
 - _ Remember that the ***RootPassword*** is case sensitive.
 - _ You are authenticated as root and returned the UNIX prompt.
- 6 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY BackupServerName:0.0**, then press **Return**.
- 7 Execute the **NetWorker Administrative** program by entering: **nwadmin**, then press **Return**.
 - _ A window opens for the **NetWorker Administrative** program.
 - _ You are now able to label tapes.
- 8 Insert the blank tape(s) in the jukebox's cartridge, then install the cartridge in the jukebox.
 - _ Remove all non-blank tapes from the cartridge.
- 9 Click the **Label** button.
 - _ The **Jukebox Labeling** window opens.
- 10 Enter **2** in the **First Slot** field, enter **11** in the **Last Slot** field.
 - _ Slot 1 is the non-removable slot within the jukebox. This usually contains a cleaning tape.
 - _ Slot 2 is at the top of the cartridge and 11 at the bottom.
 - _ It is OK to have empty slots.
- 11 Click the **OK** button.
 - _ A status message appears and updates.
 - _ Labeling a full cartridge takes about 15 minutes.
- 12 When the status in the **Jukebox Labeling** window reads finished, click the **Cancel** button.
 - _ The **Jukebox Labeling** window closes.
- 13 Go to the **File** menu, select **Exit**.
- 14 At the UNIX prompt for the ***backup server***, type **exit**, then press **Return**.
 - _ **Root** is logged out.
- 15 Type **exit** again, then press **Return**.

- You are logged out of and disconnected from the backup server.
- 16** Put a sticker on the outside of each tape cassette.
- This is done in order for you to identify it.
- 17** Resume procedure 3.2.1 or 3.2.2.

To label tapes, execute the steps provided in the following table.

Table 3.2-12. Label Tapes - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	telnet BackupServerName -or- rsh BackupServerName	press Return
2	YourUserID -or- (No entry)	press Return -or- (No action)
3	YourPassword	press Return
4	su	press Return
5	RootPassword	press Return
6	setenv DISPLAY IPNumber:0.0 -or- setenv DISPLAY BackupServerName:0.0	press Return
7	nwadmin	press Return
8	(No entry)	put blank tape(s) in cartridge and install cartridge in jukebox
9	(No entry)	click Label button
10	2	(No action)
11	11	click OK button
12	(No entry)	click Cancel button
13	File → Exit	(No action)
14	exit	press Return
15	exit	press Return
16	(No entry)	put a sticker on the outside of each tape
17	(No entry)	resume previous procedure

3.3 System Log Maintenance

The System Log Maintenance process is performed through Tivoli by the System Administrator (SA). The System Administrator will setup and execute the jobs to be run in Tivoli in various formats (i.e., reoccurring day and time, maximum amount of disk space, etc.). This section assumes that task jobs have already been created and discusses how to edit the job for System Log Maintenance.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that system log maintenance has been scheduled well in advance, all planning involved has been concluded well in advance, and the SA has been properly trained to perform all aspects of system log maintenance, and that the SA is a Tivoli administrator.

Table 3.3-1 presents the steps required to perform System Log Maintenance in a condensed manner. If you are already familiar with the procedures, you may prefer to use the quick-step tables. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

This section explains how to edit a task in Tivoli for System Log Maintenance. To begin, execute the procedure steps that follow:

- 1** Log into the **Tivoli server** by typing: **telnet *TivoliServerName* or rsh *TivoliServerName*** at the UNIX prompt, then press **Return**.
- 2** If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.
 - _ A password prompt is displayed.
- 3** Enter ***YourPassword***, then press **Return**.
 - _ Remember that ***YourPassword*** is case sensitive.
 - _ You are authenticated as yourself and returned to the UNIX prompt.
- 4** Enter **setenv DISPLAY *YourMachineName*:0.0**, then press **Return**.
- 5** Enter **tivoli**, then press **Return**.
 - _ The **TME Desktop Administrator** window appears.
- 6** Double-click on the **Scheduler** icon.
 - _ The **Scheduler Browser** window appears.
- 7** Highlight the job you wish to edit by clicking the job.
- 8** Select **Edit** from the menu at the bottom of the screen.
 - _ The **Edit Scheduled Job** window appears.
- 9** Enter all desired changes.
- 10** Select **Update & Close** from the menu at the bottom of the window.
 - _ You are logged out of and disconnected from the **TME Desktop Administrator**.
- 11** Type **exit**, then press **Return**.
 - _ You are logged out of the **Tivoli** server.

Table 3.3-1. System Log Maintenance - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	<i>YourUserID</i>	press Return
2	<i>YourPassword</i>	press Return
3	setenv DISPLAY <i>YourMachineName</i>:0.0	press Return
4	tivoli	press Return
5	(No entry)	double-click on Scheduler Icon
6	job	single-click
7	(No entry)	single-click on Edit button
8	make changes to job	
9	(No entry)	single-click on Update & Close button
10	exit	press Return

3.4 User Administration

3.4.1 Adding a User

The Adding a User process begins when the requester fills out a "User Registration Request Form" (located in Appendix A), and submits it to his/her supervisor. The "User Registration Request Form" includes information regarding the user (User's Name, Group, Organization, etc.), as well as the user's explanation of why an account on the system is needed. The requester's supervisor reviews the request, and if s/he determines that it is appropriate for the requester to have UNIX and DCE accounts, forwards the request to the Operations Supervisor (Ops Super). The Ops Super reviews the request and forwards it to the System Administrator (SA). The SA verifies that all required information is contained on the form. If it is, s/he implements the request. (Incomplete forms are returned to the requester's supervisor for additional information.) After the user is registered, the SA provides the user with a password to use for logging onto their accounts. The SA also sends an e-mail message to the user's supervisor and the Ops Super, informing them that the user's accounts were created.

The Activity Checklist table that follows provides an overview of the adding a user process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 3.4-1. Adding a User - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Complete User Registration Form and forward to his/her Supervisor.	(I) 3.4.1	
2	Super	Approve/Deny Request. If Approve, Forward Request to Ops Super.	(I) 3.4.1	
3	Ops Super	Review Request and Forward to SA.	(I) 3.4.1	
4	SA	Review User Registration Form for Completeness.	(I) 3.4.1	
5	SA	Add User.	(P) 3.4.1	
6	SA	Phone User with Password. Notify Supervisor and Ops Super that user was added.	(I) 3.4.1	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for adding a user has already been approved by DAAC Management and that the SA is a Tivoli administrator. In order to perform the procedure, the SA must have obtained the following information about the requester:

- a. **Real name of the new user**
- b. **Office number of the new user**
- c. **Office phone number of the new user**
- d. **Home phone number of the new user**
- e. **Organization**
- f. **Group affiliation(s)**
- g. **Role(s) of the new user**

Table 3.4-2 presents the steps required to add a user in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To add a new user for the requester, execute the procedure steps that follow:

- 1** At the UNIX prompt, type **tivoli**, press **Return**.
_ Tivoli starts up, and the **TME Desktop** window opens.
- 2** Double click the **Admin** Policy Region.
_ You are now able to create the account.
- 3** Double click on the **Admin_profile** icon.
_ The **Admin_profile Profile Manager** window opens.

- 4 Double click on the **users** icon.
 - The **User Profile Properties** window opens.
- 5 Click the **Add User** button.
 - The **Add Record To Profile** window opens.
- 6 Enter the *real name of the new user* in the **User Name** box, then click the **Use Defaults** button.
 - The **Add Record To Profile** window updates with the default information for the new user.
 - One of the new items of information in the **Add Record to Profile** window is the **UNIX login** for the new user. Remember what it is set to be.
 - The user's password is set to be the first initial followed by the last name. For example, if you entered a *real name of the new user* of Jane Doe then the password would be set to jdoe.
- 7 Enter the *Office Number*, *Office Telephone*, and *Home Telephone* in the corresponding fields.
- 8 Click the checkbox(es) for the new user's *Role(s)*.
- 9 Enter the new user's *Group affiliation(s)* in the **DCE Group** field, and the new user's *Organization* into the **DCE Organization** field.
- 10 Click the **Add & Close** button.
 - The UNIX and DCE accounts are created, including creation of the home directory and copying of the appropriate .cshrc file.
 - The **Add Record To Profile** window closes.
- 11 Review the **User Profile Properties** window, make sure that the new account appears in the listing.
- 12 Go to the **Profile** menu, select **Save**.
- 13 Go to the **Profile** menu, select **Distribute**.
 - The **Distribute Profile** window opens.
- 14 If any **subscribers/machines** are in the **Don't Distribute To These Subscribers** box, select them and then click the left arrow button.
 - These **subscriber(s)** will move into the **Distribute To These Subscribers** box.
- 15 Click the **Distribute & Close** button.
 - The information is distributed to the **subscriber(s)** listed in the **Distribute To These Subscribers** box.
 - The **Distribute Profile** window closes.
- 16 Return to the **TME Desktop** by closing any other open windows.

- To close the other open windows, go to the **Profile** menu in each window and select **Close**.
- 17** Double click on the **Administrators** icon.
 - The **Administrators** window opens.
- 18** Click on the new user's **Role** icon using the right mouse button, select **Edit Logins...** from the resulting menu.
 - The **Set Login Names** window opens.
- 19** Enter the **UNIX login** of the new user in the **Add Login Name** box, press **Return**.
- 20** Click the **Change & Close** button.
 - The login is added to the **Role** group.
 - The **Set Login Names** window closes.
- 21** If the new user has more than one **Role**, execute steps 18-20 for each **Role**.
- 22** Return to the **TME Desktop** by closing any other open windows.
 - To close the other open windows, go to the **Profile** menu in each window and select **Close**
- 23** Go to the **Desktop** menu, select **Quit**.
- 24** In the window that opens asking if you really want to quit, click on the **Yes** button.
 - Tivoli exits.

To add a new user, execute the steps provided in the following table.

Table 3.4-2. Add New User - Quick-Step Procedures (1 of 2)

Step	What to Enter or Select	Action to Take
1	tivoli	press Return
2	(No entry)	double click Admin Policy Region
3	(No entry)	double click Admin_profile
4	(No entry)	double click users
5	(No entry)	click Add User... button
6	<i>name of new user</i>	click Use Defaults button
7	<i>Office Number, Office Telephone, Home Telephone</i>	click checkbox(es) for the new user's Role(s)
8	<i>Group affiliation(s), Organization</i>	click Add & Close button
9	(No entry)	review User Profile Properties window, find the new account in the listing
10	Profile → Save	(No action)
11	Profile → Distribute	(No action)

Table 3.4-2. Add New User - Quick-Step Procedures (2 of 2)

Step	What to Enter or Select	Action to Take
12	any subscribers in the Don't Distribute To These Subscribers box	click the left arrow button
13	(No entry)	click Distribute & Close button
14	Profile → Quit in all windows other than the TME Desktop	double click Administrators
15	(No entry)	click on <i>Role</i> using right mouse button
16	Edit Logins...	(No action)
17	UNIX login	press Return
18	(No entry)	click Change & Close button
19	Profile → Quit in all windows other than the TME Desktop	(No action)
20	Desktop → Quit	click Yes button

3.4.2 Deleting a User

The Deleting a User process begins when the requester has determined that no useful files remain in the user's home directory and submits a request to delete the user's account to his/her supervisor. The supervisor approves or denies the request. Once approved, the request is forwarded to the Ops Super. The Ops Super reviews the request and forwards it to the SA who deletes the user's account. When the user has been deleted, the SA notifies the requester, supervisor and Ops Super.

The Activity Checklist table that follows provides an overview of the deleting a user process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 3.4-3. Deleting a User - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Determine that No Useful Files Remain in the User's Home Directory and Submit Request to his/her Supervisor.	(I) 3.4.2	
2	Super	Approve/Deny Request. If Approve, Forward Request to Ops Super.	(I) 3.4.2	
3	Ops Super	Review Request and Forward to SA.	(I) 3.4.2	
4	SA	Delete User.	(P) 3.4.2	
5	SA	Notify Requester, Supervisor and Ops Super that user was deleted.	(I) 3.4.2	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for deleting a user has already been approved by DAAC Management and that the SA is a Tivoli administrator. In order to perform the procedure, the SA must have obtained the following information from the requester:

- a. **UNIX login of the user to be deleted**
- b. **Role(s) of the user to be deleted**

Table 3.4-4 contains a table which presents the steps required to delete a user in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented in Section 3.4.2.

To delete a user for the requester, execute the procedure steps that follow:

- 1** At the UNIX prompt, type **tivoli**, press **Return**.
 - Tivoli starts up, and the **TME Desktop** window opens.
- 2** Double click the Admin Policy Region.
 - You are now able to delete the account.
- 3** Double click on the **Admin_profile** icon.
 - The **Admin_profile Profile Manager** window opens.
- 4** Double click on the **users** icon.
 - The **User Profile Properties** window opens.
- 5** Select the ***UNIX login of the user to be deleted*** in the listing.
- 6** Click the **Delete Users...** button.
 - The **Delete Home Directory Action** window opens.
- 7** Click the **Delete Home Directory** button.
 - The **Delete Home Directory Action** window closes.
 - The UNIX and DCE accounts are removed, and the user's home directory is deleted.
- 8** In the **User Profile Properties** window, go to the **Profile** menu, select **Save**.
- 9** Go to the **Profile** menu, select **Distribute**.
 - The **Distribute Profile** window opens.
- 10** If any **subscribers/machines** are in the **Don't Distribute To These Subscribers** box, select them and then click the left arrow button.
 - These **subscriber(s)** will move into the **Distribute To These Subscribers** box.
- 11** Click the **Distribute & Close** button.

- The information is distributed to the **subscriber(s)** listed in the **Distribute To These Subscribers** box.
 - The **Distribute Profile** window closes.
- 12** Return to the **TME Desktop** by closing any other open windows.
- To close the other open windows, go to the **Profile** menu in each window and select **Close**.
- 13** Double click on the **Administrators** icon.
- The **Administrators** window opens.
- 14** Click on the user's **Role** icon using the right mouse button, select **Edit Logins...** from the resulting menu.
- The **Set Login Names** window opens.
- 15** Select the *UNIX login of the user to be deleted*, then click the **Remove** button.
- 16** Click the **Change & Close** button.
- The login is removed from the **Role** group.
 - The **Set Login Names** window closes.
- 17** If the user has more than one **Role**, execute steps 14-16 for each **Role**.
- 18** Return to the **TME Desktop** by closing any other open windows.
- To close the other open windows, go to the **Profile** menu in each window and select **Close**
- 19** Go to the **Desktop** menu, select **Quit**.
- 20** In the window that opens asking if you really want to quit, click on the **Yes** button.
- Tivoli exits.

To delete a user, execute the steps provided in the following table.

Table 3.4-4. Delete a User - Quick-Step Procedures (1 of 2)

Step	What to Enter or Select	Action to Take
1	tivoli	press Return
2	(No entry)	double click Admin Policy Region
3	(No entry)	double click Admin_profile
4	(No entry)	double click users
5	<i>UNIX login of the user to be deleted</i>	click Delete Users... button
6	(No entry)	click Delete Home Directory button
7	Profile → Save	(No action)
8	Profile → Distribute	(No action)

Table 3.4-4. Delete a User - Quick-Step Procedures (2 of 2)

Step	What to Enter or Select	Action to Take
9	any subscribers in the Don't Distribute To These Subscribers box	click the left arrow button
10	(No entry)	click Distribute & Close button
11	Profile → Quit in all windows other than the TME Desktop	double click Administrators
12	(No entry)	click on <i>Role</i> using right mouse button
13	Edit Logins...	(No action)
14	UNIX login of the user to be deleted	click the Remove button
15	(No entry)	click Change & Close button
16	Profile → Quit in all windows other than the TME Desktop	(No action)
17	Desktop → Quit	click Yes button

3.4.3 Changing a User Account Configuration

The Changing a User Account Configuration process begins when the requester submits a request to the Ops Supervisor detailing what to change about the account configuration and the reason for the change. The Ops Supervisor reviews the request and forwards it to SA who changes the user's account configuration. When the changes are complete the SA notifies the requester and Ops Supervisor.

The Activity Checklist table that follows provides an overview of the changing a user account configuration process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 3.4-5. Change a User Account Configuration - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request to Ops Supervisor.	(I) 3.4.3	
2	Ops Super	Review and Forward to SA.	(I) 3.4.3	
3	SA	Change User Account Configuration.	(P) 3.4.3	
4	SA	Inform Requester and Supervisor of completion.	(I) 3.4.3	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for changing a user account configuration has already been approved by the Ops Supervisor. In order to perform the procedure, the SA must have obtained the following information from the requester:

a. **What to change and new settings.**

Can be any of:

New Real User Name

New Login ID

New Office Number

New Office Phone Number

New Home Phone Number

New UNIX Group

New DCE Group

New DCE Organization

New Login Shell

b. **Current UNIX Login of the User**

For new role(s), see procedure 3.4.4 Changing User Access Privileges. For a new home directory, see procedure 3.4.8 Moving a User's Home Directory. For a new password, see procedure 3.4.5 Changing a User Password.

Table 3.4-6 presents the steps required to change a user account configuration in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To change a user account configuration for the requester, execute the procedure steps that follow:

- 1** At the UNIX prompt, type **tivoli**, press **Return**.
_ Tivoli starts up, and the **TME Desktop** window opens.
- 2** Double click the **Admin Policy Region**.
_ You are now able to change the account configuration.
- 3** Double click on the **Admin_profile** icon.
_ The **Admin_profile Profile Manager** window opens.
- 4** Double click on the **users** icon.
_ The **User Profile Properties** window opens.

- 5 Select the *Current UNIX Login of the User* in the listing.
- 6 Click the **Edit User...** button.
 - The **Edit Profile Record** window opens.
- 7 Click the **down arrow** button next to **User Name**.
 - The **Edit Profile Record** window updates with additional information and fields.
- 8 If there is a *New Real User Name*, delete the text in the **User Name** field and then type *New Real User Name* into the **User Name** field.
- 9 If there is a *New Login ID*, delete the text in the **Login Name** field and then type *New Login ID* into the **Login Name** field.
 - Click the **down arrow** button next to **E-Mail**. Verify that the e-mail address updated properly to reflect the *New Login ID*. If it did not, delete the text in the **E-Mail** field and type in the correct new e-mail address.
- 10 If there is a *New Office Number*, delete the text in the **Office Number** field and then type *New Office Number* into the **Office Number** field.
- 11 If there is a *New Office Phone Number*, delete the text in the **Office Telephone** field and then type *New Office Phone Number* into the **Office Telephone** field.
- 12 If there is a *New Home Phone Number*, delete the text in the **Home Telephone** field and then type *New Home Phone Number* into the **Home Telephone** field.
- 13 If there is a *New UNIX Group*, delete the text in the **Primary Group** field and then type *New UNIX Group* into the **Primary Group** field.
- 14 If there is a *New DCE Group*, delete the text in the **DCE Group** field and then type *New DCE Group* into the **DCE Group** field.
- 15 If there is a *New DCE Organization*, delete the text in the **DCE Organization** field and then type *New DCE Organization* into the **DCE Organization** field.
- 16 Click the **down arrow** button next to **Login Shell**.
 - The **Edit Profile Record** window updates with additional information and fields.
- 17 If there is a *New Login Shell*, delete the text in the **Login Shell** field and then type *New Login Shell* into the **Login Shell** field.
 - The *New Login Shell* must be a full path.
- 18 Click the **Set & Close** button.
 - The user's password is changed.
 - The **Edit Profile Record** window closes.
- 19 In the **User Profile Properties** window, go to the **Profile** menu, select **Save**.
- 20 Go to the **Profile** menu, select **Distribute**.

- The **Distribute Profile** window opens.
- 21** If any **subscribers**/machines are in the **Don't Distribute To These Subscribers** box, select them and then click the left arrow button.
 - These **subscriber(s)** will move into the **Distribute To These Subscribers** box.
- 22** Click the **Distribute & Close** button.
 - The information is distributed to the **subscriber(s)** listed in the **Distribute To These Subscribers** box.
 - The **Distribute Profile** window closes.
- 23** Return to the TME Desktop by closing any other open windows.
 - To close the other open windows, go to the **Profile** menu in each window and select **Close**.
- 24** Go to the **Desktop** menu, select **Quit**.
- 25** In the window that opens asking if you really want to quit, click on the **Yes** button.
 - Tivoli exits.

To change a user account configuration, execute the steps provided in the following table.

Table 3.4-6. Change User Account Configuration - Quick-Step Procedures (1 of 2)

Step	What to Enter or Select	Action to Take
1	tivoli	press Return
2	(No entry)	double click Admin Policy Region
3	(No entry)	double click Admin_profile
4	(No entry)	double click users
5	<i>UNIX login of the user</i>	click Edit User... button
6	(No entry)	click down arrow button next to User Name
7	New Real User Name in User Name	(No action)
8	New Login ID in Login Name	click the down arrow button next to E-Mail
9	(No entry)	verify that the e-mail address updated to reflect <i>New Login ID</i>
10	New Office Number in Office Number field	(No action)
11	New Office Phone Number in Office Telephone field	(No action)
12	New Home Phone Number in Home Telephone field	(No action)
14	New UNIX Group in Primary Group field	(No action)
15	New DCE Group in DCE Group field	(No action)
16	New DCE Organization in DCE Organization field	click the down arrow button next to Login Shell
17	New Login Shell in Login Shell field	click the Set & Close button

Table 3.4-6. Change User Account Configuration - Quick-Step Procedures (2 of 2)

Step	What to Enter or Select	Action to Take
18	Profile → Save	(No action)
19	Profile → Distribute	(No action)
20	any subscribers in the Don't Distribute To These Subscribers box	click the left arrow button
21	(No entry)	click Distribute & Close button
22	Profile → Quit in all windows other than the TME Desktop	(No action)
23	Desktop → Quit	click Yes button

3.4.4 Changing User Access Privileges

The Changing User Access Privileges process begins when the requester submits a request to his/her supervisor. The supervisor approves or denies the request. Once approved, the request is forwarded to the Ops Super. The Ops Super reviews the request and forwards it to the SA who changes the user's access privileges. When the changes are complete the SA notifies the requester, supervisor and Ops Super.

The Activity Checklist table that follows provides an overview of the changing user access privileges process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 3.4-7. Changing User Access Privileges - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request to his/her Supervisor.	(I) 3.4.4	
2	Super	Approve/Deny Request. If Approve, Forward Request to Ops Super.	(I) 3.4.4	
3	Ops Super	Review Request and Forward to SA.	(I) 3.4.4	
4	SA	Change User Access Privileges.	(P) 3.4.4	
5	SA	Inform Requester, Supervisor and DAAC Mgr of completion.	(I) 3.4.4	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for changing user access privileges has already been approved by DAAC Management and that the SA is a Tivoli administrator. In order to perform the procedure, the SA must have obtained the following information about the requester:

- a. **Role(s) to which the user is to be added**
- b. **Role(s) from which the user is to be removed**
- c. **UNIX login of the user**

Table 3.4-8 presents the steps required to change user access privileges in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To change user access privileges for the requester, execute the procedure steps that follow:

- 1** At the UNIX prompt, type **tivoli**, press **Return**.
 _ Tivoli starts up, and the **TME Desktop** window opens.
- 2** Double click the Admin Policy Region.
 _ You are now able to change the user's access privileges.
- 3** Double click on the **Admin_profile** icon.
 _ The **Admin_profile Profile Manager** window opens.
- 4** Double click on the **users** icon.
 _ The **User Profile Properties** window opens.
- 5** Select the *UNIX login of the user* in the listing.
- 6** Click the **Edit User...** button.
 _ The **Edit Profile Record** window opens.
- 7** Click the **down arrow** button next to **User name**.
 _ The **Edit Profile Record** window updates with additional information.
- 8** Select the *Role(s) to which the user is to be added*, by clicking the checkbox(es) next to the role name(s).
- 9** Deselect the *Role(s) from which the user is to be removed*, by clicking the checkbox(es) next to the role name(s).
- 10** Click the **Set & Close** button.
 _ The user is added to and deleted from the designated **Role(s)**.
 _ The **Edit Profile Record** window closes.
- 11** In the **User Profile Properties** window, go to the **Profile** menu, select **Save**.
- 12** Go to the **Profile** menu, select **Distribute**.
 _ The **Distribute Profile** window opens.

- 13 If any **subscribers**/machines are in the **Don't Distribute To These Subscribers** box, select them and then click the left arrow button.
 - These **subscriber(s)** will move into the **Distribute To These Subscribers** box.
- 14 Click the **Distribute & Close** button.
 - The information is distributed to the **subscriber(s)** listed in the **Distribute To These Subscribers** box.
 - The **Distribute Profile** window closes.
- 15 Return to the **TME Desktop** by closing any other open windows.
 - To close the other open windows, go to the **Profile** menu in each window and select **Close**.
- 16 Double click on the **Administrators** icon.
 - The **Administrators** window opens.
- 17 Click on the ***Role from which the user is to be removed*** icon using the right mouse button, select **Edit Logins...** from the resulting menu.
 - The **Set Login Names** window opens.
- 18 Select the ***UNIX login of the user***, then click the **Remove** button.
- 19 Click the **Change & Close** button.
 - The login is removed from the **Role from which the user is to be removed** group.
 - The **Set Login Names** window closes.
- 20 If the user has more than one ***Role from which the user is to be removed***, execute steps 17-19 for each ***Role from which the user is to be removed***.
- 21 Click on the ***Role to which the user is to be added*** icon using the right mouse button, select **Edit Logins...** from the resulting menu.
 - The **Set Login Names** window opens.
- 22 Enter the ***UNIX login of the user*** in the **Add Login Name** box, press **Return**.
- 23 Click the **Change & Close** button.
 - The login is added to the **Role to which the user is to be added** group.
 - The **Set Login Names** window closes.
- 24 If the user has more than one ***Role to which the user is to be added***, execute steps 21-23 for each ***Role to which the user is to be added***.
- 25 Return to the **TME Desktop** by closing any other open windows.
 - To close the other open windows, go to the **Profile** menu in each window and select **Close**.
- 26 Go to the **Desktop** menu, select **Quit**.

- 27 In the window that opens asking if you really want to quit, click on the **Yes** button.
 _ Tivoli exits.

To change user access privileges, execute the steps provided in the following table.

Table 3.4-8. Change User Access Privileges - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	tivoli	press Return
2	(No entry)	double click Admin Policy Region
3	(No entry)	double click Admin_profile
4	(No entry)	double click users
5	<i>UNIX login of the user</i>	click Edit User... button
6	(No entry)	click down arrow button next to User name
7	Role(s) to which the user is to be added	deselect Role(s) from which the user is to be removed
8	(No entry)	click the Set & Close button
9	Profile → Save	(No action)
10	Profile → Distribute	(No action)
11	any subscribers in the Don't Distribute To These Subscribers box	click the left arrow button
12	(No entry)	click Distribute & Close button
13	Profile → Quit in all windows other than the TME Desktop	double click Administrators
14	(No entry)	click on Role from which the user is to be removed using right mouse button
15	Edit Logins...	(No action)
16	<i>UNIX login of the user</i>	click the Remove button
17	(No entry)	click Change & Close button
18	(No entry)	click on Role to which the user is to be added using right mouse button
19	Edit Logins...	(No action)
20	<i>UNIX login of the user</i>	press Return
21	(No entry)	click Change & Close button
22	Profile → Quit in all windows other than the TME Desktop	(No action)
23	Desktop → Quit	click Yes button

3.4.5 Changing a User Password

The Changing a User Password process begins when the requester submits a request to the SA. The SA verifies that the requester is who s/he claims to be. Once verified, the SA changes the user's password. When the change is complete the SA notifies the requester.

The Activity Checklist table that follows provides an overview of the changing a user password process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 3.4-9. Changing a User Password - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request to SA.	(I) 3.4.5	
2	SA	Verify that the Requester is Who S/he Claims to Be.	(I) 3.4.5	
3	SA	Change Password.	(P) 3.4.5	
4	SA	Inform Requester of completion.	(I) 3.4.5	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for changing a user password has already been approved by DAAC Management and that the SA is a Tivoli administrator. In order to perform the procedure, the SA must have obtained the following information about the requester:

- a. **UNIX login of the user**
- b. **New password for the user**

Table 3.4-10 presents the steps required to change a user password in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To change a user password for the requester, execute the procedure steps that follow:

- 1** At the UNIX prompt, type **tivoli**, press **Return**.
 _ Tivoli starts up, and the **TME Desktop** window opens.
- 2** Double click the **Admin** Policy Region.
 _ You are now able to delete the account.
- 3** Double click on the **Admin_profile** icon.
 _ The **Admin_profile Profile Manager** window opens.
- 4** Double click on the **users** icon.

- The **User Profile Properties** window opens.
- 5 Select the *UNIX login of the user* in the listing.
- 6 Click the **Edit User...** button.
 - The **Edit Profile Record** window opens.
- 7 Click the **down arrow** button next to **Password**.
 - The **Edit Profile Record** window updates with additional information.
- 8 Type the *New password for the user* in the **Password** field.
 - You will not be able to read what you type in this field.
 - Remember that the *New password for the user* is case sensitive.
- 9 Click the **Set & Close** button.
 - The user's password is changed.
 - The **Edit Profile Record** window closes.
- 10 In the **User Profile Properties** window, go to the **Profile** menu, select **Save**.
- 11 Go to the **Profile** menu, select **Distribute**.
 - The **Distribute Profile** window opens.
- 12 If any **subscribers/machines** are in the **Don't Distribute To These Subscribers** box, select them and then click the left arrow button.
 - These **subscriber(s)** will move into the **Distribute To These Subscribers** box.
- 13 Click the **Distribute & Close** button.
 - The information is distributed to the **subscriber(s)** listed in the **Distribute To These Subscribers** box.
 - The **Distribute Profile** window closes.
- 14 Return to the **TME Desktop** by closing any other open windows.
 - To close the other open windows, go to the **Profile** menu in each window and select **Close**.
- 15 Go to the **Desktop** menu, select **Quit**.
- 16 In the window that opens asking if you really want to quit, click on the **Yes** button.
 - Tivoli exits.

To change a user password, execute the steps provided in the following table.

Table 3.4-10. Change User Password - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	tivoli	press Return
2	(No entry)	double click Admin Policy Region
3	(No entry)	double click Admin_profile
4	(No entry)	double click users
5	UNIX login of the user	click Edit User... button
6	(No entry)	click down arrow button next to Password
7	New password for the user	click the Set & Close button
8	Profile → Save	(No action)
9	Profile → Distribute	(No action)
10	any subscribers in the Don't Distribute To These Subscribers box	click the left arrow button
11	(No entry)	click Distribute & Close button
12	Profile → Quit in all windows other than the TME Desktop	(No action)
13	Desktop → Quit	click Yes button

3.4.6 Checking a File/Directory Access Privilege Status

The Checking a File/Directory Access Privilege Status process begins when the requester submits a request to the SA. The SA checks the file/directory access privilege status and reports the status back to the requester.

The Activity Checklist table that follows provides an overview of the checking a file/directory access privilege status process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 3.4-11. Checking a File/Directory Access Privilege Status - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit a Request to the SA.	(I) 3.4.6	
2	SA	Check a File/Directory Access Privilege Status.	(P) 3.4.6	
3	SA	Inform Requester of completion and Report the File/Directory Access Privilege Status.	(I) 3.4.6	

Detailed procedures for tasks performed by the SA are provided in the sections that follow. In order to perform the procedure, the SA must have obtained the following information about the requester:

a. **full path of the file/directory on which privilege status is needed**

Table 3.4-12 contains a table which presents the steps required to check a file/directory access privilege status in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To check a file/directory access privilege status for the requester, execute the procedure steps that follow:

1 At a UNIX prompt, type **cd *Path***, press **Return**.

- The ***Path*** is the full path up to but not including the file/directory on which access privilege status is needed. For example, if the requester wants access privileges status on directory /home/jdoe then type **cd /home** and press **Return**.

2 Type **ls -la | grep *FileOrDirectoryName***, press **Return**.

- This command will return information like this:
drwxr-xr-x 19 jdoe user 4096 Jun 28 09:51 jdoe
-r-xr--r-- 1 jdoe user 80 Jun 22 11:22 junk

What this output means, from left to right, is:

- The file type and access permissions:
 - The first character indicates what type of file it is:
A d means that the file is a directory.
A - means that the file is an ordinary file.
A l means that the file is a symbolic link.
 - The next three characters indicate the user/owner privileges, in the order of read, write and then execute. r=read, w=write and x=execute. A - is used as a place holder. For example the owner of the second file (junk) does not have write permissions, so a - appears rather than a w as the third character in the line.
 - The next three characters indicate the group privileges, in the order of read, write and then execute. r=read, w=write and x=execute. A - is used as a place holder. For example the group of the first file/directory (jdoe) does not have write permissions, so a - appears rather than a w as the sixth character in the line.
 - The next three characters indicate the privileges that everyone else/other has, in the order of read, write and then execute. r=read, w=write and x=execute. A - is used as a place holder. For example, other in the case of the first file/directory (jdoe) does not have write permissions, so a - appears rather than a w as the ninth character in the line.

- There are 19 links to this file/directory.
- The owner of the file/directory is jdoe.
- The file/directory's group is user.
- The file/directory is 4096 bytes large.
- The last time that the file/directory was modified is Jun 28 at 09:51.
- The name of the file/directory is jdoe.

3 Create a report of the file/directory's access privilege status by using the information produced by step 2 and by filling out this template:

full path of the file/directory: _____

owner: _____

group: _____

owner/user privileges: _____ **read** _____ **write** _____ **execute**

group privileges: _____ **read** _____ **write** _____ **execute**

everyone else/other privileges: _____ **read** _____ **write** _____ **execute**

To check a file/directory access privilege status, execute the steps provided in the following table.

Table 3.4-12. Check a File/Directory Access Privilege Status - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	<code>cd Path</code>	press Return
2	<code>ls -la grep FileOrDirectoryName</code>	press Return
3	(No entry)	generate a file/directory access privilege status report

3.4.7 Changing a File/Directory Access Privilege

The Changing a File/Directory Access Privilege process begins when the requester submits a request to his/her supervisor to have file/directory access privileges changed. The supervisor approves/denies the request. When approved, the request is forwarded to the Ops Supervisor who reviews the request and forwards it to the SA. The SA changes the file/directory access privileges and then notifies the requester, supervisor and Ops Supervisor of completion.

The Activity Checklist table that follows provides an overview of the changing a file/directory access privilege process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 3.4-13. Changing a File/Directory Access Privilege - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request to his/her Supervisor.	(I) 3.4.7	
2	Super	Approve/Deny Request. If Approve, Forward Request to Ops Supervisor.	(I) 3.4.7	
3	Ops Super	Review Request and Forward to SA.	(I) 3.4.7	
4	SA	Change a File/Directory Access Privilege.	(P) 3.4.7	
5	SA	Inform Requester, Supervisor and Ops Supervisor of completion.	(I) 3.4.7	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for changing a file/directory access privilege has already been approved by his/her supervisor. In order to perform the procedure, the SA must have obtained the following information about the requester:

- a. **full path of the file/directory on which access privileges will be changed**
- b. **new access privileges to set on the file/directory. Can be any of:**
 - New owner**
 - New group**
 - New user/owner privileges (read, write and/or execute)**
 - New group privileges (read, write and/or execute)**
 - New other privileges (read, write and/or execute)**

Table 3.4-14 contains a table which presents the steps required change a file/directory access privilege in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To change a file/directory access privilege for the requester, execute the procedure steps that follow:

- 1 At the UNIX prompt, type **su**, press **Return**.
- 2 At the **Password** prompt, type **RootPassword**, press **Return**.
 - Remember that **RootPassword** is case sensitive.
 - You are authenticated as root.
- 3 Type **cd Path**, press **Return**.
 - The **Path** is the full path up to but not including the file/directory on which access privileges will be changed. For example, if the requester wants access privileges changed on directory /home/jdoe then type **cd /home** and press **Return**.
- 4 If there is a **New owner** then type **chown NewOwner FileOrDirectoryName**, press **Return**.
 - The **FileOrDirectoryName** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type **chown NewOwner jdoe** and press **Return**.
- 5 If there is a **New group** then type **chgrp NewGroup FileOrDirectoryName**, press **Return**.
 - The **FileOrDirectoryName** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type **chgrp NewGroup jdoe** and press **Return**.
- 6 If there are **New user/owner privileges** then type **chmod u=NewUserPrivileges FileOrDirectoryName**, press **Return**.
 - The **FileOrDirectoryName** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type **chmod u=NewUserPrivileges jdoe**, press **Return**.
 - The **NewUserPrivileges** are r for read, w for write and x for execute. For example, to give the user/owner read, write and execute privileges, type **chmod u=rwx FileOrDirectoryName** and press **Return**.
- 7 If there are **New group privileges** then type **chmod g=NewGroupPrivileges FileOrDirectoryName**, press **Return**.
 - The **FileOrDirectoryName** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type

chmod g=NewGroupPrivileges jdoe, press **Return**.

- The *NewGroupPrivileges* are r for read, w for write and x for execute. For example, to give the group read and execute privileges, type **chmod g=rx FileOrDirectoryName** and press **Return**.

8 If there are **New other privileges** then type **chmod o=NewOtherPrivileges FileOrDirectoryName**, press **Return**.

- The *FileOrDirectoryName* is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type **chmod o=NewOtherPrivileges jdoe**, press **Return**.

- The *NewOtherPrivileges* are r for read, w for write and x for execute. For example, to give other read privileges, type **chmod o=r FileOrDirectoryName** and press **Return**.

9 Type **exit**, press **Return**.

- Root is logged out.

To change a file/directory access privilege, execute the steps provided in the following table.

Table 3.4-14. Change a File/Directory Access Privilege - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	su	press Return
2	RootPassword	press Return
3	cd Path	press Return
4	chown NewOwner FileOrDirectoryName	press Return
5	chgrp NewGroup FileOrDirectoryName	press Return
6	chmod u=NewUserPrivileges FileOrDirectoryName	press Return
7	chmod g=NewGroupPrivileges FileOrDirectoryName	press Return
8	chmod o=NewOtherPrivileges FileOrDirectoryName	press Return
9	exit	press Return

3.4.8 Moving a User's Home Directory

The Moving a User's Home Directory process begins when the requester submits a request to the Ops Supervisor. The Ops Supervisor approves or denies the request. Once approved, the request is forwarded to the SA who moves the user's home directory. When the changes are complete the SA notifies the requester and Ops Supervisor.

The Activity Checklist table that follows provides an overview of moving a user's home directory process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task.

Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 3.4-15. Moving a User's Home Directory - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request to Ops Supervisor.	(I) 3.4.8	
2	Ops Super	Approve/Deny Request in Accordance with Policy. Forward to SA if approved.	(I) 3.4.8	
3	SA	Move a User's Home Directory.	(P) 3.4.8	
4	SA	Inform Requester and Ops Super of completion.	(I) 3.4.8	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for moving a user's home directory has already been approved by DAAC Management and that the SA is a Tivoli administrator. In order to perform the procedure, the SA must have obtained the following information about the requester:

- a. **UNIX login of the user**
- b. **New location for home directory**

Table 3.4-16 presents the steps required to move a user's home directory in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To move a user's home directory for the requester, execute the procedure steps that follow:

- 1** At the UNIX prompt, type **tivoli**, press **Return**.
_ Tivoli starts up, and the **TME Desktop** window opens.
- 2** Double click the **Admin** Policy Region.
_ You are now able to delete the account.
- 3** Double click on the **Admin_profile** icon.
_ The **Admin_profile Profile Manager** window opens.
- 4** Double click on the **users** icon.
_ The **User Profile Properties** window opens.
- 5** Select the **UNIX login of the user** in the listing.

- 6 Click the **Edit User...** button.
 - The **Edit Profile Record** window opens.
- 7 Click the **down arrow** button next to **Home Directory**.
 - The **Edit Profile Record** window updates with additional information.
- 8 When prompted with **If changing user's home directory:**, choose **Move contents of old home directory to new one** by clicking this radio button.
- 9 Type *New location for home directory* in the **Home Directory Path** field.
 - The **New location for home** directory must be a full path.
- 10 Click the **Set & Close** button.
 - The user's home directory is moved.
 - The **Edit Profile Record** window closes.
- 11 In the **User Profile Properties** window, go to the **Profile** menu, select **Save**.
- 12 Go to the **Profile** menu, select **Distribute**.
 - The **Distribute Profile** window opens.
- 13 If any **subscribers**/machines are in the **Don't Distribute To These Subscribers** box, select them and then click the left arrow button.
 - These **subscriber(s)** will move into the **Distribute To These Subscribers** box.
- 14 Click the **Distribute & Close** button.
 - The information is distributed to the **subscriber(s)** listed in the **Distribute To These Subscribers** box.
 - The **Distribute Profile** window closes.
- 15 Return to the **TME Desktop** by closing any other open windows.
 - To close the other open windows, go to the **Profile** menu in each window and select **Close**.
- 16 Go to the **Desktop** menu, select **Quit**.
- 17 In the window that opens asking if you really want to quit, click on the **Yes** button.
 - Tivoli exits.

To move a user's home directory, execute the steps provided in the following table.

Table 3.4-16. Move a User's Home Directory - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	tivoli	press Return
2	(No entry)	double click Admin Policy Region
3	(No entry)	double click Admin_profile
4	(No entry)	double click users
5	<i>UNIX login of the user</i>	click Edit User... button
6	(No entry)	click down arrow button next to Home Directory
7	Move contents of old home directory to new one	(No action)
8	<i>New location for home directory</i>	click Set & Close button
9	Profile → Save	(No action)
10	Profile → Distribute	(No action)
11	any subscribers in the Don't Distribute To These Subscribers box	click the left arrow button
12	(No entry)	click Distribute & Close button
13	Profile → Quit in all windows other than the TME Desktop	(No action)
14	Desktop → Quit	click Yes button

3.5 Installing a New Workstation

The Installing a New Workstation process has three stages - preparation, installation and testing, and verification. The preparation stage begins with the System Administrator (SA) performing procedure 3.5.1.1 Hardware Preparation. Once the hardware is prepared, the SA continues on and prepares for network configuration, procedure 3.5.1.2.

The next stage is installation which begins by reporting the hardware to inventory, procedure 3.5.2.1.1. The SA continues this stage by installing the operating system, procedure 3.5.2.2. Installation is then completed by installing custom software, procedure 3.5.2.3.1, and installing COTS software, procedure 3.5.2.3.2.

The final stage is testing and verification. The SA begins this stage by rebooting the machine, procedure 3.5.3.1. The testing and verification is completed by logging in, procedure 3.5.3.2, and testing the environment, procedure 3.5.3.3.

The Activity Checklist table that follows provides an overview of the New Workstation Installation process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 3.5-1. Installing a New Workstation - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Prepare Hardware	(P) 3.5.1.1	
2	SA	Prepare for Network Configuration	(P) 3.5.1.2	
3	SA	Report Hardware to Inventory	(P) 3.5.2.1.1	
4	SA	Install Operating System	(P) 3.5.2.2	
5	SA	Install Custom Software	(P) 3.5.2.3.1	
6	SA	Install COTS Software	(P) 3.5.2.3.2	
7	SA	Reboot	(P) 3.5.3.1	
8	SA	Log In	(P) 3.5.3.2	
9	SA	Test Environment	(P) 3.5.3.3	

3.5.1 Preparation

3.5.1.1 Hardware Preparation

The Hardware Preparation process begins when the requester submits a request to the SA. The SA then determines if the requested hardware is on hand or must be ordered. Once the hardware is available along with all the necessary attachments, the SA will schedule the installation. After the Hardware Preparation is complete, the SA proceeds to procedure 3.5.1.2, Network Configuration.

The Activity Checklist table that follows provides an overview of the Hardware Preparation process. column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 3.5-2. Hardware Preparation - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Make request known to Operation Supervisor	(I) 3.5.1.1	
2	Operations Supervisor	Submit a request to the DAAC Manager for approval	(I) 3.5.1.1	
3	DAAC Manager	Submit approved request to the SA	(I) 3.5.1.1	
4	SA	Determine if the requested hardware is on hand or must be ordered.	(I) 3.5.1.1	
5	SA	Schedule the Installation.	(I) 3.5.1.1	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the hardware installation has been scheduled well in advance, all planning involved has been concluded well in advance and the SA has been properly trained to install the hardware. The SA must obtain the following information from the requester:

- a. **type of hardware desired (HP, Sun, SGI or NCD)**
- b. **location of installation**

Refer to Section 3.3 of the Release A Installation Plan (800-TP-005-001) for detailed instruction on how to install hardware.

3.5.1.2 Network Configuration

The Network Configuration process begins after section 3.5.1.1 Hardware Preparation has been completed in the Installing a New Workstation process. Once complete, the SA proceeds to procedure 3.5.2.1.1 Reporting to Inventory.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that procedure 3.5.1.1 Hardware Preparation has been completed and that the SA has been properly trained in network configuration.

Table 3.5-3 presents the steps required to prepare for network configuration in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

The following steps are required to prepare for network configuration:

- 1** Determine the name of the hardware.
 - For example, if the hardware is a NCD, the name will be ncd# where # is sequential from the inventory list. If the hardware is a Sun, the name may be personalized (i.e., fred).
- 2** Submit a request to the Network Administrator for the IP address and the DNS entry.

NOTE: If the hardware is a NCD, the SA needs to determine the name of the NCD Login Host. The NCD Login Host will be the name of the X-server this NCD will use.

To prepare for network configuration, execute the steps provided in the following table.

Table 3.5-3. Prepare for Network Configuration - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	determine name of workstation
2	(No entry)	determine NCD Login Host
3	(No entry)	submit request to Network Administrator for IP address and DNS entry

3.5.2 Installation

3.5.2.1 Hardware

3.5.2.1.1 Reporting to Inventory

The Reporting to Inventory process begins after the SA has completed Section 3.5.1.1 Hardware Preparation and 3.5.1.2 Network Configuration. After the Reporting to Inventory is complete, the SA proceeds to procedure 3.5.2.2 Operating System Installation.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that procedures 3.5.1.1 and 3.5.1.2 have been completed.

Table 3.5-4 presents the steps required to report to inventory in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

The following steps are required to report to inventory:

- 1** Locate the Inventory Control Number on each hardware component and record them.
 - The Inventory Control Number is on a small bright sticker on the front of each hardware component.
- 2** Submit the Inventory Control Numbers and location of the machine to the Inventory Controller.

To report to inventory, execute the steps provided in the following table.

Table 3.5-4. Report to Inventory - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	locate and record the Inventory Control Numbers
2	(No entry)	report the Inventory Control Numbers and location of the machine to the Inventory Controller

3.5.2.2 Operating System Installation - By Operating System Type

3.5.2.2.1 Solaris 2.4 Operating System Installation

Solaris 2.4 is also known as Sun OS 5.4. The Solaris 2.4 Operating System Installation process begins when procedure 3.5.2.1 Installation of Hardware has been completed in the Installing a New Workstation process. Once complete, the SA proceeds to procedure 3.5.2.3.1 Installation of Custom Software.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedure assumes that procedures 3.5.1 Preparation and 3.5.2.1 Installation of Hardware have been completed. The procedure also assumes that the workstation is powered off.

Table 3.5-5 presents the steps required to install the Solaris 2.4 operating system in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

This section explains how to install the Solaris 2.4 operating system, including network configuration and patch installation. If you would like a listing of the patches installed, please see document number 420-TD-012-001 Release A Sun Solaris Operating System Patch List attached at the end of this document. To install the Solaris 2.4 operating system, execute the procedure steps that follow:

- 1 Get the download disk.
- 2 Check that the download disk is set to be target 2.
 - Facing the front of the download disk, the target number is found on the back, to the right on the disk.
 - You can change the target number by hitting the pins above and below it.
- 3 Plug the download disk into the Sun.
- 4 Power on the download disk.
 - Facing the front of the disk, the power switch is found on the back, to the left on the disk.
- 5 Power on the monitor, power on the Sun.
 - The Sun's power switch is located on the back of the Sun. When facing the front of the Sun, the power switch is on the right.
- 6 At the > prompt, type **probe-scsi**, press **Return**.
 - Verify that target 2 exists by finding it in the listing that appears.
- 7 Type **boot disk2 -swr**, press **Return**.
 - The Sun boots up.
 - s is for single user, w is for writeable and r is for reconfigure (required because you added a drive).
- 8 Type **RootPassword**, press **Return**.
 - **RootPassword** is the root password for the download disk.
 - Remember that the **RootPassword** is case sensitive.
 - You are authenticated as root and returned the UNIX prompt.
- 9 Type **/download/setup**, press **Return**.

- Status messages will be displayed.
- 10 When prompted for the Sun's name, type *SunsName*, press **Return**.
- 11 When prompted for the Sun's IP address, type *SunsIP*, press **Return**.
 - The Sun's network and hostname are configured.
- 12 When you are returned to a UNIX prompt, type */etc/halt*, press **Return**.
- 13 At the > prompt, power off the download disk.
- 14 Disconnect the download disk from the Sun.
- 15 At the > prompt, type **boot -r**, press **Return**.
 - The Sun boots up.
 - r is for reconfigure (required because you removed a drive).
- 16 At the **login:** prompt, type **root**, press **Return**.
- 17 Type *RootPassword*, press **Return**.
 - *RootPassword* is the root password for the download disk. (The Sun uses the download disk's root password until a new one is set.)
 - Remember that the *RootPassword* is case sensitive.
 - You are authenticated as root and returned the UNIX prompt.
- 18 Type **passwd root**, press **Return**.
- 19 At the **New password:** prompt, type *RootPassword*, press **Return**.
 - *RootPassword* is the root password for the Sun.
 - Remember that the *RootPassword* is case sensitive.
- 20 At the **Re-enter new password:** prompt, type *RootPassword*, press **Return**.
 - *RootPassword* is the root password for the Sun.
 - This step confirms that the root password has been entered correctly.
 - Remember that the *RootPassword* is case sensitive.
 - The root password for this Sun is set. Inform all authorized personnel of *RootPassword*.
- 21 Type **exit**, press **Return**.
 - Root is logged out of the Sun.
- 22 Inform the backup administrator of the new machine.

To install the Solaris 2.4 operating system, execute the steps provided in the following table.

Table 3.5-5. Install the Solaris 2.4 Operating System - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	get the download disk
2	(No entry)	check that download disk is set to target 2
3	(No entry)	plug download disk into Sun
4	(No entry)	power on download disk
5	(No entry)	power on monitor
6	(No entry)	power on Sun
7	probe-scsi	press Return
8	(No entry)	verify that target 2 exists
9	boot disk2 -swr	press Return
10	<i>RootPassword of download disk</i>	press Return
11	/download/setup	press Return
12	<i>SunsName</i>	press Return
14	<i>SunsIP</i>	press Return
15	/etc/halt	press Return
16	(No entry)	power off download disk
17	(No entry)	disconnect download disk from Sun
18	boot -r	press Return
19	root	press Return
20	<i>RootPassword of download disk</i>	press Return
21	passwd root	press Return
22	<i>RootPassword for the Sun</i>	press Return
23	<i>RootPassword for the Sun</i>	press Return
24	exit	press Return
25	(No entry)	inform all authorized personnel of <i>RootPassword for the Sun</i>
26	(No entry)	inform backup administrator of new Sun

3.5.2.2.2 HP-UX 9.05 Operating System Installation

The HP-UX 9.05 Operating System Installation process begins when procedure 3.5.2.1 Installation of Hardware has been completed in the Installing a New Workstation process. Once complete, the SA proceeds to procedure 3.5.2.3.1 Installation of Custom Software.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedure assumes that procedures 3.5.1 Preparation and 3.5.2.1 Installation of Hardware have been completed. The procedure also assumes that the workstation is powered off.

Table 3.5-6 presents the steps required to install the HP-UX 9.05 operating system in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

This section explains how to install the HP-UX 9.05 operating system, including network configuration and patch installation. If you would like a listing of the patches installed, please see document number 420-TD-014-001 Release A HP Operating System Patch List attached at the end of this document. To install the HP-UX 9.05 operating system, execute the procedure steps that follow:

- 1 Get the download disk.
- 2 Check that it is set to be target 2.
 - _ The target number is found on the back of the disk.
 - _ You can change the target number by hitting the buttons above and below it.
- 3 Plug the download disk into the HP.
- 4 Power on the download disk.
 - _ The power switch is located on the back of the drive.
- 5 Power on the monitor, power on the HP.
 - _ The power switch is located on the right side of the HP, towards the front.
 - _ The HP starts booting up.
- 6 At the **Selecting a system to boot. To stop selection process press and hold the ESCAPE key** message, press and hold **Escape**.
 - _ You have 10 seconds to press **Escape** before the boot process proceeds.
 - _ The boot process will stop and a menu of boot commands will appear.
- 7 Select boot scsi.2.0 by typing **b DeviceSelectionForscsi.2.0 isl**, press **Return**.
 - _ For example, if the Device Selection for scsi.2.0 in the menu is P1 then type **b P1 isl** and then press **Return**.
 - _ **isl** will cause the HP to boot in interactive mode.
- 8 At the **ISL>** prompt, type **hpux -is boot disk(scsi.2;0)/hp-ux**, press **Return**.
 - _ **-is** causes the HP to boot in single user mode.
 - _ You will be returned to the UNIX prompt.
- 9 Type **/download/setup**, press **Return**.
 - _ Status messages will be displayed.
- 10 When prompted for the HP's name, type **HPsName**, press **Return**.
- 11 When prompted for the HP's IP address, type **HPsIP**, press **Return**.
 - _ The HP's network and hostname are configured.
- 12 When you are returned to a UNIX prompt, type **/etc/shutdown -h -y now**, press **Return**.
 - _ The HP shuts down and comes to a halt.

- 13 Once the HP has halted, power off the download disk, power off the monitor.
- 14 Power off the HP.
- 15 Disconnect the download disk from the HP.
- 16 Power on the monitor.
- 17 Power on the HP.
 - The HP starts booting up.
- 18 At the **Selecting a system to boot. To stop selection process press and hold the ESCAPE key** message, press and hold **Escape**.
 - You have 10 seconds to press **Escape** before the boot process proceeds.
 - The boot process will stop and a menu of boot commands will appear.
- 19 Select boot scsi.6.0 by typing **b DeviceSelectionForscsi.6.0**, press **Return**.
 - For example, if the Device Selection for scsi.6.0 in the menu is P1 then type **b P1** and press **Return**.
- 20 At the **login:** prompt, type **root**, press **Return**.
- 21 Type **RootPassword**, press **Return**.
 - **RootPassword** is the root password for the download disk. (The HP uses the download disk's root password until a new one is set.)
 - Remember that the **RootPassword** is case sensitive.
 - You are authenticated as root and returned the UNIX prompt.
- 22 Type **passwd root**, press **Return**.
- 23 At the **New password:** prompt, type **RootPassword**, press **Return**.
 - **RootPassword** is the root password for the HP.
 - Remember that the **RootPassword** is case sensitive.
- 24 At the **Re-enter new password:** prompt, type **RootPassword**, press **Return**.
 - **RootPassword** is the root password for the HP.
 - This step confirms that the root password has been entered correctly.
 - Remember that the **RootPassword** is case sensitive.
 - The root password for this HP is set. Inform all authorized personnel of **RootPassword**.
- 25 Type **exit**, press **Return**.
 - Root is logged out of the HP.
- 26 Inform the backup administrator of the new machine.

To install the HP-UX 9.05 operating system, execute the steps provided in the following table.

Table 3.5-6. Install the HP-UX 9.05 Operating System - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	get the download disk
2	(No entry)	check that download disk is set to target 2
3	(No entry)	plug download disk into HP
4	(No entry)	power on download disk
5	(No entry)	power on monitor
6	(No entry)	power on HP
7	(No entry)	press and hold Escape
8	b DeviceSelectionForscsi.2.0 isl	press Return
9	hpux -is boot disk(scsi.2;0)/hp-ux	press Return
10	/download/setup	press Return
11	HPsName	press Return
12	HPsIP	press Return
14	/etc/shutdown -h -y now	press Return
15	(No entry)	power off download disk
16	(No entry)	power off the monitor
17	(No entry)	power off the HP
18	(No entry)	disconnect download disk from HP
19	(No entry)	power on the monitor
20	(No entry)	power on the HP
21	(No entry)	press and hold Escape
22	b DeviceSelectionForscsi.6.0	press Return
23	root	press Return
24	RootPassword of download disk	press Return
25	passwd root	press Return
26	RootPassword for the HP	press Return
27	RootPassword for the HP	press Return
28	exit	press Return
29	(No entry)	inform all authorized personnel of <i>RootPassword for the HP</i>
30	(No entry)	inform backup administrator of new HP

3.5.2.2.3 IRIX 5.3 and 6.2 Operating Systems Installation

The IRIX 5.3 and 6.2 Operating Systems Installation process begins when procedure 3.5.2.1 Installation of Hardware has been completed in the Installing a New Workstation process. Once complete, the SA proceeds to procedure 3.5.2.3.1 Installation of Custom Software.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedure assumes that procedures 3.5.1 Preparation and 3.5.2.1 Installation of Hardware have been completed. The procedure also assumes that the workstation is powered off.

Table 3.5-7 presents the steps required to install the IRIX 5.3 and 6.2 operating systems in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

This section explains how to install the IRIX 5.3 and 6.2 operating systems, including network configuration and patch installation. If you would like a listing of the patches installed for IRIX 5.3, please see document number 420-TD-013-001 Release A SGI Irix 5.3 Operating System Patch List attached at the end of this document.

To install the IRIX 5.3 or 6.2 operating system, execute the procedure steps that follow:

- 1 Get the download disk.
- 2 Check that it is set to be target 2.
 - _ The target number is found on the bottom of the disk.
 - _ You can change the target number by hitting the buttons above and below it.
- 3 Plug the download disk into the SGI.
- 4 Power on the download disk.
 - _ The power switch is located on the back of the drive.
- 5 Power on the monitor; power on the SGI.
 - _ The power switch is located on the front of the SGI, towards the left.
- 6 At the **Starting up the system...** message, click the **Stop for Maintenance** button.
 - _ You have only a few seconds to click the **Stop for Maintenance** button before the boot process proceeds.
 - _ The boot process will stop and a **System Maintenance** menu will appear.
- 7 Select **5 Enter Command Monitor**.
 - _ You will be returned to the Command Monitor prompt which is >>.
- 8 At the >> prompt, type **hinv**, press **Return**.
 - _ Verify that target 2 exists by finding it in the listing that appears. It will appear as **SCSI Disk: scsi(0)disk(2)**.
- 9 Type **boot -f dksc(0,2,0)sash**, press **Return**.
 - _ The SGI boots from the download disk into the stand alone shell.
 - _ You will be returned to a UNIX prompt.
- 10 Type **/download/setup**, press **Return**.
 - _ Status messages will be displayed.
- 11 When prompted for the SGI's name, type **SGIsName**, press **Return**.

- 12 When prompted for the SGI's IP address, type *SGIsIP*, press **Return**.
 - The SGI's network and hostname are configured.
 - 13 When you are returned to a UNIX prompt, type */etc/shutdown -y -g0*, press **Return**.
 - The SGI shuts down.
 - You will be returned to a >> prompt, a **System Maintenance** menu or a message saying that **this system can be powered off**.
 - 14 Power off the download disk, power off the monitor.
 - 15 Power off the SGI.
 - 16 Disconnect the download disk from the SGI.
 - 17 Power on the monitor.
 - 18 Power on the SGI.
 - The SGI starts booting up.
 - 19 At the **login:** prompt, type **root**, press **Return**.
 - 20 Type *RootPassword*, press **Return**.
 - *RootPassword* is the root password for the download disk. (The SGI uses the download disk's root password until a new one is set.)
 - Remember that the *RootPassword* is case sensitive.
 - You are authenticated as root and returned the UNIX prompt.
 - 21 Type **passwd root**, press **Return**.
 - 22 At the **New password:** prompt, type *RootPassword*, press **Return**.
 - *RootPassword* is the root password for the SGI.
 - Remember that the *RootPassword* is case sensitive.
 - 23 At the **Re-enter new password:** prompt, type *RootPassword*, press **Return**.
 - *RootPassword* is the root password for the SGI.
 - This step confirms that the root password has been entered correctly.
 - Remember that the *RootPassword* is case sensitive.
 - The root password for this SGI is set. Inform all authorized personnel of *RootPassword*.
 - 24 Type **exit**, press **Return**.
 - Root is logged out of the SGI.
 - 25 Inform the backup administrator of the new machine.
- To install the IRIX 5.3 or 6.2 operating system, execute the steps provided in the following table.

Table 3.5-7. Install the IRIX 5.3 or 6.2 Operating System - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	get the download disk
2	(No entry)	check that download disk is set to target 2
3	(No entry)	plug download disk into SGI
4	(No entry)	power on download disk
5	(No entry)	power on monitor
6	(No entry)	power on SGI
7	(No entry)	click the Stop for Maintenance button
8	5 Enter Command Monitor	(No action)
9	hinv	press Return
10	(No entry)	verify that SCSI Disk: scsi(0)disk(2) appears in the listing
11	boot -f dksc(0,2,0)sash	press Return
12	/download/setup	press Return
13	<i>SGIsName</i>	press Return
14	<i>SGIsIP</i>	press Return
15	/etc/shutdown -y -g0	press Return
16	(No entry)	power off download disk
17	(No entry)	power off monitor
18	(No entry)	power off SGI
19	(No entry)	disconnect download disk from SGI
20	(No entry)	power on monitor
21	(No entry)	power on SGI
22	root	press Return
23	<i>RootPassword of download disk</i>	press Return
24	passwd root	press Return
25	<i>RootPassword for the SGI</i>	press Return
26	<i>RootPassword for the SGI</i>	press Return
27	exit	press Return
28	(No entry)	inform all authorized personnel of <i>RootPassword for the SGI</i>
29	(No entry)	inform backup administrator of new SGI

3.5.2.2.4 NCD Operating System Installation

The NCD Operating System Installation process begins when procedure 3.5.2.1 Installation of Hardware has been completed in the Installing a New Workstation process. Once complete, the SA proceeds to procedure 3.5.3 Testing and Verification.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedure assumes that procedures 3.5.1 Preparation and 3.5.2.1 Installation of Hardware have been completed. The procedure also assumes that the workstation is powered off.

Installing the NCD operating system consists of configuring the NCD.

Table 3.5-8 presents the steps required to configure the NCD in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

This section explains how to configure the NCD, including putting the necessary start-up files in place on the server.

To configure the NCD, execute the procedure steps that follow:

- 1** Turn on the NCD and monitor. The monitor power button is on the lower front of the monitor. The NCD power switch is on the back, on the right.
 - The message **Boot Monitor Vx.x.x** will appear.
- 2** Press the **Escape** key twice.
 - You have only a few seconds to press the **Escape** key.
 - The boot process stops and a boot monitor prompt, **>**, appears.
 - If you do not see a **>** prompt then press the **Escape** key a few more times.
- 3** Press the **Setup** key.
 - The **Main** menu will appear.
- 4** Go to the **Keyboard** menu by pressing the **Right Arrow** key.
 - The **Keyboard** menu appears.
- 5** Select **N-101** by pressing the **Down Arrow** key.
 - You may need to press the **Down Arrow** key a few times before **N-101** is selected.
- 6** Go to the **Monitor** menu by pressing the **Right Arrow** key.
 - The **Keyboard** menu disappears.
 - The **Monitor Resolution** menu appears.
- 7** Select **1600x1200 65 Hz** by pressing the **Down Arrow** key.
 - You may need to press the **Down Arrow** key a few times before **1600x1200 65 Hz** is selected.
- 8** Press the **Shift** and **T** keys.
 - This tests the new monitor resolution setting.
- 9** Use the **+** and **-** keys on the front of the monitor under the **ADJUST** label to adjust the screen.
- 10** Press the **STORE** key on the front of the monitor.
 - The monitor stores the screen adjustments.
- 11** Press the **Escape** key.

- The monitor resolution test ends.
 - You are returned to the **Main** menu.
- 12 Go to the **Network** menu by pressing the **Right Arrow** key twice.
 - The **Monitor Resolution** menu disappears.
 - The **Network** menu appears.
- 13 Select **NVRAM** for the **Get IP Addresses From** option.
 - You can use the **Space Bar** to move between the available options.
- 14 Press the **Down Arrow** key.
- 15 Type the *NCDIPaddress* for the **Terminal IP Address** option, press the **Down Arrow** key.
 - The *NCDIPaddress* is in dotted decimal notation, for example, 155.157.21.34.
- 16 Type the *StartupFileServerIPaddress* for the **First Boot Host IP Address** option, press the **Down Arrow** key.
 - The *StartupFileServerIPaddress* is in dotted decimal notation, for example, 155.157.44.22.
 - The *StartupFileServer* is the machine where the NCD startup files are stored.
- 17 Press the **Down Arrow** key twice.
- 18 Type the *NCDGatewayIPaddress* for the **Gateway IP address** option, press the **Down Arrow** key.
 - The *NCDGatewayIPaddress* is in dotted decimal notation, for example, 155.157.44.22.
 - The *NCDGatewayIPaddress* is the same as the *NCDIPaddress* except the last number/octet is 1. For example, if the *NCDIPaddress* is 155.157.21.34, the *NCDGatewayIPaddress* is 155.157.21.1.
- 19 Press the **Down Arrow** key, type the *BroadcastIPaddress* for the **Broadcast IP Address** option.
 - The *BroadcastIPaddress* is in dotted decimal notation, for example, 155.157.44.22.
 - The *BroadcastIPaddress* is the same as the *NCDIPaddress* except the last number/octet is 255. For example, if the *NCDIPaddress* is 155.157.21.34, the *BroadcastIPaddress* is 155.157.21.255.
- 20 Press the **Right Arrow** key.
 - The **Network** menu disappears.
 - The **Boot** menu appears.
- 21 Type *Xncdhmx_s* for the **Boot File** option, press the **Down Arrow** key.
- 22 Press the **Down Arrow** key, type */data/ncd/* for the **NFS Boot Directory** option, press the **Down Arrow** key.

- 23 Press the **Down Arrow** key, type `/usr/lib/X11/ncd/configs/` for the **UNIX Config Directory** option, press the **Down Arrow** key.
- 24 Press the **Down Arrow** key, press the **d** key.
_ The **TFTP Order** option is set to **Disabled**.
- 25 Press the **Down Arrow** key, press the **1** key.
_ The **NFS Order** option is set to **1**.
- 26 Press the **Down Arrow** key, press the **d** key.
_ The **MOP Order** option is set to **Disabled**.
- 27 Press the **Down Arrow** key, press the **d** key.
_ The **LOCAL Order** option is set to **Disabled**.
- 28 Press the **Right Arrow** key.
_ The **Boot** menu disappears.
_ The **Done** menu appears.
_ **Reboot** is selected.
- 29 Press the **Return** key.
_ The NCD reboots.
_ Status messages appear.
- 30 Log into the *StartupFileServer* by typing: **telnet StartupFileServer** or **rsh StartupFileServer** at a UNIX prompt, then press **Return**.
- 31 If a **Login:** prompt appears, log in as yourself by typing: *YourUserID*, then press **Return**.
_ A password prompt is displayed.
- 32 Enter *YourPassword*, then press **Return**.
_ Remember that *YourPassword* is case sensitive.
_ You are authenticated as yourself and returned to the UNIX prompt.
- 33 Log in as root by typing: **su**, then press **Return**.
_ A password prompt is displayed.
- 34 Enter the *RootPassword*, then press **Return**.
_ Remember that the *RootPassword* is case sensitive.
_ You are authenticated as root and returned to the UNIX prompt.
- 35 Type **cd /usr/lib/X11/ncd/configs**, press **Return**.
- 36 Type **./i**, press **Return**.
_ **i** is a script which builds a NCD startup file.

- 37 Type the last two numbers/octets of the *NCDIPaddress* when the script prompts you for the **IP address**, press **Return**.
 _ For example, if the *NCDIPaddress* is 155.157.21.34 then type **21.34** and then press **Return**.
- 38 Type the *NCDLoginHost* when the script prompts you for the **Login Host**, press **Return**.
 _ The *NCDLoginHost* is the name of one of the X-servers.
- 39 When the script prompts you for the **NCD Number**, type the *NCDname* minus the “ncd” part.
 _ For example, if the *NCDname* is ncd2 then the **NCD Number** is 2.
 _ Some status messages appear telling you what the script is doing.
 _ The script exits.
- 40 Type **exit**, then press **Return**.
 _ **Root** is logged out
- 41 Type **exit** again, then press **Return**.
 _ You are logged out and disconnected from the *StartupFileServer*.

To configure the NCD, execute the steps provided in the following table.

Table 3.5-8. Configure the NCD - Quick-Step Procedures (1 of 2)

Step	What to Enter or Select	Action to Take
1	(No entry)	power on the monitor and NCD
2	(No entry)	press Escape twice
3	(No entry)	press Setup key
4	(No entry)	press Right Arrow key
5	N-101	press Right Arrow key
6	1600x1200 65 Hz	press Shift and T keys
7	(No entry)	use + and - keys under ADJUST on front of monitor to adjust the screen
8	(No entry)	press the STORE key on the front of the monitor
9	(No entry)	press Escape
10	(No entry)	press Right Arrow key twice
11	NVRAM	press Down Arrow key
12	<i>NCDIPaddress</i>	press Down Arrow key
13	<i>StartupFileServerIPaddress</i>	press Down Arrow key three times
14	<i>NCDGatewayIPaddress</i>	press Down Arrow key twice
15	<i>BroadcastIPaddress</i>	press Right Arrow key
16	Xncdhmx_s	press Down Arrow key twice
17	/data/ncd/	press Down Arrow key twice

Table 3.5-8. Configure the NCD - Quick-Step Procedures (2 of 2)

Step	What to Enter or Select	Action to Take
18	/usr/lib/X11/ncd/configs/	press Down Arrow key twice
19	(No entry)	press d key
20	(No entry)	press Down Arrow key
21	(No entry)	press 1 key
22	(No entry)	press Down Arrow key
23	(No entry)	press d key
24	(No entry)	press Down Arrow key
25	(No entry)	press d key
26	(No entry)	press Right Arrow key
27	(No entry)	press Return
28	telnet <i>StartupFileServer</i> -or- rsh <i>StartupFileServer</i>	press Return
29	<i>YourUserID</i>	press Return
30	<i>YourPassword</i>	press Return
31	su	press Return
32	<i>RootPassword</i>	press Return
33	cd /usr/lib/X11/ncd/configs	press Return
34	./i	press Return
35	last two numbers/octets of <i>NCDIPAddress</i>	press Return
36	<i>NCDLoginHost</i>	press Return
37	<i>NCDname</i> minus the "ncd" part	press Return
38	exit	press Return
39	exit	press Return

3.5.2.3 Software

3.5.2.3.1 Custom

The Installation of Custom Software process begins when procedure 3.5.2.2 Operating System Installation has been completed in the Installing a New Workstation process. Once complete, the SA proceeds to procedure 3.5.2.3.2 Installation of COTS Software.

Detailed procedures for tasks performed by the SA are provided below. The procedure assumes that procedures 3.5.1 Preparation, 3.5.2.1 Installation of Hardware and 3.5.2.2 Operating System Installation have been completed.

Table 3.5-9 presents the steps required to install custom software in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To install custom software for the requester, execute the procedure step that follows:

- 1 execute procedures in Section 22.2.3 Custom Software Installation in this document.

To install custom software, execute the steps provided in the following table.

Table 3.5-9. Install Custom Software - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	execute procedures in Section 22.2.3 of this document

3.5.2.3.2 COTS

The COTS Software Installation process begins after the SA has completed Section 3.5.2.3.1 Custom Software Installation. After the COTS software installation is complete, the SA proceeds to procedure 3.5.3 Testing and Verification.

Detailed procedures for tasks performed by the SA are provided below. The procedure assumes that procedures 3.5.1 Preparation, 3.5.2.1 Installation of Hardware, 3.5.2.2 Operating System Installation and 3.5.2.3.1 Custom Software Installation have been completed.

Table 3.5-10 contains a table which presents the steps required to install COTS software in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To install COTS software for the requester, execute the procedure steps that follow:

- 1 Refer to the Release A Hardware and Software Mapping Baseline (attached at the end of this document) for your site.
 - For LaRC, refer to document number 420-TD-007-001.
 - For SMC, refer to document number 420-TD-008-001.
 - For GSFC, refer to document number 420-TD-006-001.
- 2 In the Release A Hardware and Software Mapping Baseline for your site, look up which COTS packages need to be installed on the new workstation using the **Subsystem** and hardware type (the **Target Operating System** column in the document) of the new machine.

To install COTS software, execute the steps provided in the following table.

Table 3.5-10. Install COTS Software - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	refer to the Release A Hardware and Software Mapping Baseline for your site
2	(No entry)	look up which COTS packages to install using the Subsystem and Target Operating System of the new workstation

3.5.3 Testing and Verification

3.5.3.1 Reboot

The Reboot process begins when procedure 3.5.2.3.2 COTS - By Package has been completed in the Installing a New Workstation process. Once complete, the SA proceeds to procedure 3.5.3.2 Logging In.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that procedures 3.5.1 Preparation and 3.5.2 Installation have been completed.

Table 3.5-11 presents the steps required to reboot in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

3.5.3.1.1 SGI, HP and Sun

To reboot, execute the procedure steps that follow:

- 1 At the UNIX prompt for the workstation, type **su**, press **Return**.
- 2 At the **Password** prompt, type **RootPassword**, press **Return**.
 - Remember that **RootPassword** is case sensitive.
 - You are authenticated as root.
- 3 Type **who**, press **Return**.
 - A list of users currently logged into the workstation appears.
- 4 If users other than root and you are logged in:
 - type **wall**,
 - press **Return**,
 - type **The system is going down in 5 minutes for Reason. Please save your work and log off. We apologize for the inconvenience.**

press **Return**,
 press **Control-D**,
 wait 5 minutes before proceeding to step 5.

- 5 Type **/etc/reboot**, then press **Return**.
 - The workstation reboots.
 - Watch the status messages that appear for any errors.
 - If you are returned to a **Login** prompt and saw no errors during the reboot, the reboot was successful.
 - If the reboot was unsuccessful, use the error messages and system logs to figure out what is incorrect in the workstation installation. The system logs are:
 /var/adm/messages for Solaris 2.4/5.4, /var/adm/SYSLOG for IRIX 5.3 and 6.2, and /usr/adm/syslog and rc.log for HP-UX 9.05.

To reboot, execute the steps provided in the following table.

Table 3.5-11. Reboot - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	su	press Return
2	RootPassword	press Return
3	who	press Return
4	wall	press Return
5	The system is going down in 5 minutes for <i>Reason</i> . Please save your work and log off. We apologize for the inconvenience.	press Return
6	(No entry)	press Control-D
7	(No entry)	wait 5 minutes
8	/etc/reboot	press Return
9	(No entry)	watch for errors in the boot messages

3.5.3.1.2 NCD

The Reboot the NCD process begins when procedure 3.5.2.3.2 COTS - By Package has been completed in the Installing a New Workstation process. Once complete, the SA proceeds to procedure 3.5.3.2 Logging In.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that procedures 3.5.1 Preparation and 3.5.2 Installation have been completed.

Table 3.5-12 presents the steps required to reboot the NCD in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To reboot the NCD, execute the procedure steps that follow:

- 1** Press the **Setup** key.
 - The **NCD User Services: Console** window will appear.
- 2** Go to the **Console** menu, select **Reboot**.
 - The **Reboot** window opens asking if it is **OK to reboot the terminal**.
- 3** Click the **OK** button.
 - The NCD reboots.
 - Watch the status messages that appear.
 - Once the NCD successfully reboots, a login screen appears.
 - If the NCD does not successfully reboot then use the information in the status messages to determine what went wrong in procedure 3.5.2.2.4 NCD Operating System Installation.

To reboot the NCD, execute the steps provided in the following table.

Table 3.5-12. Reboot the NCD - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	press Setup key
2	Console → Reboot	click OK button
3	(No entry)	watch for errors in the boot messages

3.5.3.2 Logging In

The Logging In process begins when procedure 3.5.3.1 Reboot has been completed in the Installing a New Workstation process. Once complete, the SA proceeds to procedure 3.5.3.3 Test Environment.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that procedures 3.5.1 Preparation, 3.5.2 Installation and 3.5.3.1 Reboot have been completed. The procedures also assume that the workstation is currently at a **Login** prompt.

Table 3.5-13 presents the steps required to log in in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To log in, execute the procedure steps that follow:

- 1** At the **Login** prompt for the workstation, type **YourUserID**, press **Return**.

- 2 At the **Password** prompt, type *YourPassword*, press **Return**.
 - Remember that *YourPassword* is case sensitive.
 - You are logged in and authenticated as yourself.
 - You are returned to a UNIX prompt.
 - If you are not logged in and returned to a UNIX prompt, logging in was unsuccessful. Follow these steps:
 - a Execute this procedure one more time.
 - If logging in is unsuccessful again, there is a problem with the workstation installation. Continue to step b.
 - b Type **root** at the **Login** prompt, press **Return**.
 - c Type *RootPassword* at the **Password** prompt, press **Return**.
 - Remember that *RootPassword* is case sensitive.
 - You are authenticated as root and returned to a UNIX prompt.
 - d Check that automount is running by typing **ps -ef | grep auto** or **ps -aux | grep auto**, press **Return**.
 - If automount is running then you will see output similar to this:


```
yourID 10173 0.2 0.4 648 408 pts/38 S 15:35:51 0:00 grep auto
root   140    0.0 0.8 1796 1004 ?      S Jun 25  2:40 /usr/lib/autofs/
                                automountd -D ARCH=sun5
```
 - If automount is not running then run it by typing:

/usr/lib/autofs/automountd -D ARCH=sun5 for Solaris 2.4/5.4,

/usr/etc/automount -D ARCH=sgi for IRIX 5.3 and 6.2,

/usr/etc/automount -D ARCH=hp for HP-UX 9.05,

press **Return**.

Try logging in again by typing **su - YourUserID**, press **Return**,

type *YourPassword*, press **Return**. Type **whoami** and press **Return** to

confirm that you successfully logged in as yourself and type **cd**, press

Return, type **pwd**, press **Return** to confirm that you are in your home

directory. If these commands return *YourUserID* and your home directory,

you have successfully logged in. If you have not successfully logged in,

proceed to step e.
 - e The workstation probably did not successfully bind to a NIS server. Verify that
 the NIS server is up and on the network. Once it is, execute procedure 3.5.3.1

Reboot and then execute this procedure again.

To log in, execute the steps provided in the following table.

Table 3.5-13. Log In - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	<i>YourUserID</i>	press Return
2	<i>YourPassword</i>	press Return

3.5.3.3 Test Environment

The Test Environment process begins when procedure 3.5.3.2 Logging In has been completed in the Installing a New Workstation process. Once the test environment procedure is complete, the Installing a New Workstation process is complete and the SA notifies the requester, his/her supervisor and the DAAC Manager.

The Activity Checklist table that follows provides an overview of the test environment process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 3.5-14. Test Environment - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Test Environment.	(P) 3.5.3.3.1	
2	SA	Inform Requester, Supervisor and DAAC Manager of completion.	(I) 3.5.3.3.1	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that procedures 3.5.1 Preparation, 3.5.2 Installation, 3.5.3.1 Reboot and 3.5.3.2 Logging In have been completed.

Table 3.5-15 presents the steps required to test the environment in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To test the environment, execute the procedure steps that follow:

- 1 At the UNIX prompt, type **ps -ef | more** or **ps -aux | more**.
 - A screen full of information about the currently running processes is displayed.
- 2 Look for the processes associated with the custom and COTS software which you installed in the process listing.
 - To move to the next page full of information, press the **Space** bar.
 - If a process is missing in the listing, go back to the installation of that software package to determine what went wrong.
- 3 Type **cd ~/YourUserID**, press **Return**.
- 4 Type **pwd**, press **Return**, use the output to verify that you are in your home directory.

- This verifies that automount is running and working correctly for the NIS map auto.home. You may follow steps similar to steps 3 and 4 for the other NIS maps.
- This also verifies that the new workstation was able to contact a NIS server.

To test the environment, execute the steps provided in the following table.

Table 3.5-15. Test Environment - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	ps -ef -or- ps -aux	press Return
2	(No entry)	find processes associated with the installed custom and COTS software packages in the listing
3	(No entry)	press Space bar for the next page of process information
4	cd ~/YourUserID	press Return
5	pwd	press Return
6	(No entry)	use the output to verify that you are in your home directory

3.6 DCE Configuration

3.6.1 Configuring Initial Cell

The Configuring the Initial Cell consists of configuring the Master Security Server, initial CDS Server and DTS Servers (Time & Time Provider servers). This section describes how to configure the Master Security server and initial CDS server. Section 3.6.2 explains setting up the DTS server(s).

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that all planning involved has been concluded well in advance and the SA has been properly trained to perform the configuration.

Table 3.6-1 presents the steps required to configure the initial cell in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

This section explains how to configure the initial cell. To begin configuring the initial cell, execute the procedures steps that follow:

NOTE: When planning a DCE cell, note that you must configure a CDS client on any Security server system that is not running a CDS server. You must also configure a Time client on any system that is not running a Time server. Be sure to configure these clients only after you have configured all servers.

- 1 Log in as root on the system you wish to configure
- 2 Make sure that /etc is in your command search path:
#export PATH=/etc:\$PATH (Bourne/Korn shell)
% setenv PATH /etc:\$PATH (C shell)
- 3 Type in the following appropriate command:
The sun command is dcesetup config client
The IBM command is mkdce -a cell_admin
-s edf-bb.gsfc.nasa.gov -c edf-bb.gsfc.nasa.gov cds_cl
The HP OSF DCE command is dce_config
Example:
<baltic /home/reginald>dce_config (HP OSF DCE command)
- 4 From the DCE Main Menu, select “configure and start DCE deamons” (selection 1).
- 5 From the DCE Configuration Menu, select “Initial Cell Configuration” (selection 1).
- 6 From the Initial Cell Configuration Menu, select “Security Server” (selection 1).
- 7 If this is your very first cell configuration, or if you have previously run REMOVE, answer **n** to the following question. If you are re-configuring a cell, answer **y**.
Do you wish to first remove all remnants of previous DCE configurations for all components (y/n)?
You should do so only if you plan on re-configuring all existing DCE components now: (n)
- 8 Enter the name of your cell (without /.../).
dce_config will prompt you with a warning. If rpcd was recently running with the TCP protocol sequence, then wait until 4 minutes have elapsed since rpcd was stopped before continuing from this prompt:
- 9 Enter keyseed for initial database master key:
- 10 dce_config prompts you to choose the Cell Administrators' principal name and password. The default principle name for the Cell Administrator is cell_admin:
- 11 dce_config prompts you for the starting point for UNIX user and group ID's that will be generated by the DCE Security Service. This step prevents the DCE Security Service from generating IDs that are already in use by your system. Type <RETURN> to choose the default value, or enter a value of our choice:

- 12 Enter the starting point to be used for UNIX ID'S that are automatically generated by the Security Service when a principal is added using "rgy_edit": (N +100) <RETURN>

This system is now configured as the Master Security server. You must now create a CDS server, either on this system or on another system.

If the CDS server for this cell will be on another system, repeat the steps 1-4 above on that system, then continue with Step 13.

If the CDS server is on the same system as the Security server, continue with Step 14 below.

- 13 From the DCE Configuration Menu, select "Initial Cell Configuration" (selection 1)
- 14 From the Initial Cell Configuration menu, choose "Initial CDS Server" (selection 2)
This routine starts up cdsadv and cdsd, initializes the namespace, and sets ACLs for all new namespace entries.
- 15 dce_config asks if your cell resides on multiple LAN's. If your cell does reside on multiple LAN's, dce_config asks for the name of the LAN. The name you provide is arbitrary, and is used by dce_config to store cell profile information.

Table 3.6-1. Configuring Initial Cell - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	Login as root
2	(No entry)	Make sure that /etc is in your command search path
3	(No entry)	type appropriate setup command
4	(No entry)	select 1 from DCE Main Menu
5	(No entry)	select 1 from the DCE Configuration Menu
6	(No entry)	select 1 from the Cell Configuration Menu
7	(No entry)	If reconfiguring, answer yes. If not reconfiguring, answer no.
8	(No entry)	Enter cell name
9	(No entry)	Enter keyseed.
10	(No entry)	Enter principal name and password.
11	(No entry)	Press <return> for default or enter a value.
12	(No entry)	Press <return> or enter value
13	(No entry)	select 1 from DCE Configuration Menu
14	(No entry)	select 2 from Initial Initial Cell Configuration Menu
15	(No entry)	Enter arbitrary LAN name.

3.6.2 Configuring DTS Servers

The Configuring the DTS Servers process begins after the Master CDS server has been configured. Refer to section 3.6.1 Configuring Initial Cell for Master CDS Server Configuration procedures before continuing with this section.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that all planning involved has been concluded well in advance and the SA has been properly trained to perform the configuration.

Table 3.6-2 presents the steps required to configure DTS servers in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

This section explains how to configure the DTS daemon. To begin configuring the DTS daemon, execute the procedures steps that follow:

NOTE: To configure a DTS server on a system not already configured as a Security or Directory server, repeat steps 1-4 of section 3.6.1.1 (Configuring the Initial Cell) on that system, and then continue with the steps below. To configure a DTS server on a system already configured as a Security or Directory server, continue with step 1 below.

- 1** From the DCE Configuration menu, select “Additional Server Configuration” (selection 2).
- 2** From the Additional Server Configuration menu, select “DTS” (selection 2).
- 3** From the DTS Configuration menu, select DTS Local Server for servers on the LAN (selection 1). Otherwise, select DTS global server (selection 2). Either selection starts the dts daemon (dtsd) and dtstimed.
- 4** Configure a DTS time provider on one of the time servers in a cell. Select the DTS Time Provider (selection 4).

The DTS null time provider configures a system to trust its own clock as an accurate source of time. The DTS ntp provider obtains an accurate source of time from some other system outside the cell. See the OSF DCE Administration Guide for more information on time providers.

- 5** From the DTS Time Provider Menu, select Null Time Provider (selection 1) or NTP Time Provider (selection 2).

If you select the NTP time provider the following prompt appears: Enter the host name where the NTP server is running:

- 6** Enter the host name.

Table 3.6-2. Configuring DTS Servers - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	select 2 from DCE Configuration Menu
2	(No entry)	select 2 from Additional Server Configuration Menu
3	(No entry)	select 1 for servers on the same LAN or select 2 from the DTS Configuration Menu
4	(No entry)	select 4 to configure DTS time provider
5	(No entry)	select 1 or 2 from DTS Time Provider Menu
6	(No entry)	enter the host name where the NTP server is running

3.6.3 Configuring Additional CDS Servers

The Configuring Additional CDS Servers process begins after the DTS servers have been configured. Refer to section 3.6.2 procedures before continuing with this section.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that all planning involved has been concluded well in advance and the SA has been properly trained to perform the configuration.

Table 3.6-3 presents the steps required to configure additional CDS servers in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

This section explains how to configure additional CDS servers. To begin configuring the additional CDS servers, execute the procedures steps that follow:

- 1 From the DCE Configuration menu, select “Additional Server Configuration” (selection 2).
- 2 Enter the name of your cell.
- 3 Enter the host name of your cell’s security server.

Make sure the contents of the pe_site file is identical on both the server and the client. The dce_config script checks this, but prompts for your confirmation. Identical pe_site files are normally generated automatically, but you should confirm this yourself, particularly during your initial set-up. If the pe_site files are not identical, you should start this procedure again.

Ensure the /opt/dcelocal/etc/security/pe_site file matches that on the server...

- 4 Press <RETURN> to continue, CTRL-C to exit: <RETURN>

- 5 Enter the cell administrator's principal name and password.
- 6 From the Additional Server Configuration menu, select Additional CDS Server(s) (selection 1).
- 7 Enter the name of the cell CDS server. If the cell has more than one CDS server, choose one.
- 8 dce_config asks if more directories should be replicated. If you answer **yes**, continue to step 9.
- 9 Enter a list of directories to be replicated, separated by spaces and terminated by <RETURN>.

Notes on Configuring Additional CDS Servers

Immediately after configuring an additional CDS server, you should skulk the root directory using the set directory `./:` to skulk command as `cell_admin` in `cdscp`. This will initiate the propagation of a consistent copy of the changed root directory information to all the CDS servers, and will prevent problems which might arise from use of inconsistent information before this propagation. The use of several CDS servers may increase the time required to complete the propagation of this information.

Configuration of additional CDS servers can occasionally fail if namespace information is not correctly propagated. Typical failures observe from this cause are:

ERROR: Error during creation of clearinghouse `./:/nodename_ch`.

Message from `cdscp`:

Failure in routine: `cp_create_clh`; code = 282109010

Requested operation would result in lost connectivity to root directory
(`dce / cds`)

ERROR: Error during creation of clearinghouse `./:/nodename_ch`.

Message from `cdscp`:

Failure in routine: `cp_create_clh`; code = 282108908

Unable to communicate with any CDS server (`dce / cds`)

If this happens, the server daemon `cdsd` has been successfully launched, but its clearinghouse has not been properly created. The clearinghouse is in an intermediate state and cannot be used or deleted, although the rest of the cell namespace and other servers are unaffected. To recover, skulk the root directory, and then use the `create clearinghouse ./:/nodename_ch` command as `cell_admin` in `cdscp` on the new CDS server node to manually complete the configuration of the new server and its clearinghouse. Then skulk the root directory again.

In rare circumstances, you may see the following error when configuring a CDS client or additional server:

ERROR: cdscp error during "define cached server" command.

Message from cdscp:

Failure in routine: cp_define_cached_server; code = 282111142

Cached Server clearinghouse already exists (dce / cds)

This error is benign and results from the system trying to repeat an operation that has already been done. This error may be ignored.

Table 3.6-3. Configuring Additional CDS Servers - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	select 2 from the DCE Configuration menu
2	(No entry)	Enter the name of your cell
3	(No entry)	Enter the host name of your cell's security server
4	(No entry)	press <return> to continue or CTRL-C to exit
5	(No entry)	Enter the cell administrator's principal and password
6	(No entry)	select 1 from the Additional Server Configuration menu
7	(No entry)	Enter the name of the cell CDS server
8	(No entry)	answer "yes" and continue to step 9 or answer "no" to end process
9	(No entry)	Enter a list of directories to be replicated

3.6.4 Configuring Security and CDS Client Systems

Before configuring clients, configure server systems as described in the Initial Cell Configuration, Configuring DTS Servers, and Configuring Additional CDS Servers sections. Then use this procedure to configure client systems.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that all planning involved has been concluded well in advance and the SA has been properly trained to perform the configuration.

Table 3.6-4 presents the steps required to configure security and CDS client systems in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

This section explains how to configure security and CDS client systems. To begin configuring the security and CDS client systems, execute the procedures steps that follow:

You must configure a CDS client on any Security server system that is not running a CDS server. To configure a client system, you need to know the name of the Security server and the initial CDS server for the cell.

Note that this procedure does not create a DTS clerk (client). This is described in section 3.6.5.

- 1 Start dce_config on the system that you wish to configure with DCE client(s).
- 2 From the DCE Main menu, select “Configure” (selection 1).
- 3 From the DCE Configuration menu, select “DCE Client” (selection 3).
- 4 Enter the name of your cell.
- 5 Enter the name of the security server for the cell. Then press <RETURN> to continue, CTRL-C to exit: <RETURN>
- 6 Enter the cell administrator’s principal name and password.
- 7 Enter the name of a CDS server in this cell. If there is more than one, first enter the name of the server to be cached, if necessary. Then continue with the next server(s).

You will be asked whether or not this node is to be configured as a DFS client. Answer **no**.
- 8 You will now be asked to create a LAN profile so clients and servers can be divided into profile groups for higher performance in a multi-lan cell. Answer **no**.
- 9 You will now be asked if this machine should be configured as a DTS Clerk, DTS Local Server or DTS Global Server (the default is DTS Clerk). Type **local**.

Table 3.6-4. Configuring Security and CDS Client Systems - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	start dce_config
2	(No entry)	select 1 from DCE Main menu
3	(No entry)	select 3 from DCE Configuration menu
4	(No entry)	Enter the name of your cell
5	(No entry)	Enter the name of the security server for the cell
6	(No entry)	Enter the cell administrator’s principal name and password
7	(No entry)	Enter the name of a CDS server in this cell
8	(No entry)	answer “no” for the node to be configured as a DFS client
9	(No entry)	type “local” for DTS Local Server

3.6.5 Configuring DTS Clerks

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that all planning involved has been concluded well in advance and the SA has been properly trained to perform the configuration.

Table 3.6-5 presents the steps required to configure DTS clerks in a condensed manner. If you are already familiar with the procedures, you may prefer to use the quick-step tables. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

This section explains how to configure DTS clerks. To begin configuring the DTS clerks, execute the procedures steps that follow:

You must configure a DTS clerk (client) on any system not running a DTS server. A DTS clerk is not started automatically via the dce_config “DCE Client” menu option; you must explicitly start a DTS clerk from the “DTS” menu under “Additional Server Configuration”.

- 1 Start dce_config on the system that you wish to configure with a DTS clerk.
- 2 From the DCE Main menu, select “Configure” (selection 1).
- 3 From the DCE Configuration menu, select “Additional Server Configuration” (selection 2).
- 4 From the Additional Server Configuration menu, select “DTS” (selection 2).
- 5 From the DTS Configuration menu, select “DTS Clerk” (selection 3).

This node is now a DTS clerk.

Table 3.6-5. Configuring DTS Clerks - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	start dce_config
2	(No entry)	select 1 from DCE Main menu
3	(No entry)	select 2 from DCE Configuration menu
4	(No entry)	select 2 from Additional Server Configuration menu
5	(No entry)	select 3 from DTS Configuration menu

3.6.6 Configuring GDA Servers

The DCE Global Directory Agent (GDA) facilitates communication between DCE cells. This section describes how to start the GDA server. A GDA server can only be configured on an existing client system or CDS server system.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that all planning involved has been concluded well in advance and the SA has been properly trained to perform the configuration.

Table 3.6-6 presents the steps required to configure GDA servers in a condensed manner. If you are already familiar with the procedures, you may prefer to use the quick-step tables. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

This section explains how to configure GDA servers. To begin configuring the GDA servers, execute the procedures steps that follow:

- 1** From the DCE Main menu, select “Configure” (selection 1).
- 2** From the DCE Configuration menu, select “Additional Server Configuration” (selection 2).
- 3** From the Additional Server Configuration menu, select “GDA Server” (selection 7).

The system configures the GDA server and starts the GDA server daemon, gdad.

Table 3.6-6. Configuring GDA Servers - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	select 1 from DCE Main menu
2	(No entry)	select 2 from DCE Configuration menu
3	(No entry)	select 7 from Additional Server Configuration menu

3.6.7 Creating Security Server Replica

A new feature of HP DCE/9000 is Security Server Replication, which provides for improved cell performance and reliability. These steps will allow you to create a security replica via dce_config.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that all planning involved has been concluded well in advance and the SA has been properly trained to perform the configuration.

Table 3.6-7 presents the steps required to create a security server replica in a condensed manner. If you are already familiar with the procedures, you may prefer to use the quick-step tables. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

This section explains how to create a security server replica. To begin creating a security server replica, execute the procedures steps that follow:

- 1 From the DCE Main menu, select “Configure” (selection 1).
- 2 From the DCE Configuration menu, select “Additional Server Configuration” (selection 2).
- 3 From the Additional Server Configuration menu, select “Replica Security Server” (selection 8).
- 4 Enter the keyseed for the initial database master key.

The default name for the replica is `subsys/dce/sec/$HOSTNAME`. If you wish to change the name of the security replica that is created by `dce_config`, change the value of `SEC_REPLICA`, either in the file `/opt/dcelocal/etc/dce_com_env` or in the shell environment from which `dce_config` is run. Note that you must do this before running `dce_config`.

Table 3.6-7. Creating a Security Server Replica - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	select 1 from DCE Main menu
2	(No entry)	select 2 from DCE Configuration menu
3	(No entry)	select 8 from Additional Server Configuration menu
4	(No entry)	Enter keyseed for initial database master key

3.6.8 Unconfiguring DCE Client

The UNCONFIGURE option removes the target machine from the cell Security database and the CDS namespace. DCE daemons must be running on the system executing the UNCONFIGURE option. If daemons have been stopped, use the START option on the DCE Main Menu to restart them before using UNCONFIGURE. A successfully configured client system can be unconfigured locally. If there were any errors in configuring the client system as a security or directory service client, then the client must be unconfigured from some other system in the cell. Do not use the UNCONFIGURE option on a system that is used as a Security server or a CDS server. The UNCONFIGURE option removes the system from a cell. If the system is used as a Security server or a CDS server, UNCONFIGURE will break the cell.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that all planning involved has been concluded well in advance and the SA has been properly trained to perform the configuration.

Table 3.6-8 present the steps required to unconfigure a DCE client in a condensed manner. If you are already familiar with the procedures, you may prefer to use the quick-step tables. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

This section explains how to Unconfigure a DCE Client. To begin Unconfiguring DCE Client, execute the procedures steps that follow:

- 1 From the DCE Main menu, select “Unconfigure” (selection 4).
 - 2 Enter the host name of the node to be unconfigured.
 - 3 Unconfiguring a node will remove the node’s ability to operate in the cell. A reconfiguration of the node will be required.
 - 4 You will be asked if you wish to continue. Type “y” to continue.
 - 5 Enter the Cell Administrator’s principal name and password.
- WARNING: A dce_config REMOVE will need to be performed from node baltic before reconfiguring it.
- 6 From the DCE Main menu, select “Remove” (selection).
- Remove will remove the node’s ability to operate in the cell. A reconfiguration of the node will be required. If this is not a server node, then this node should be unconfigured before a REMOVE is done.
- 7 You will again be asked if you wish to continue. Type “y” to continue.
 - 8 From the DCE Configuration menu, select “Exit” (selection 99).

You have now exited from dce_config.

Table 3.6-8. Unconfiguring DCE Client - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	select 4 from DCE Main menu
2	(No entry)	enter host name of node to be configured
3	(No entry)	type “y” to continue
4	(No entry)	enter Cell Administrator’s principal name and password
5	(No entry)	select 5 from DCE Main menu
6	(No entry)	type “y” to continue
7	(No entry)	select 99 from DCE Configuration menu

4. Database Administration

4.1 The Role of the Database Administrator (DBA)

The Database Administrator or DBA, is the individual or office responsible for the installation, configuration, update, maintenance, and overall performance and reliability of the SQL Server database. In general, the DBA is concerned with the availability of the server, the definition and management of resources allocated to the server, the definition and management of databases and objects resident on the server, and the relationship between the server and the operating system.

Each section in this chapter provides necessary background information, followed by step-by-step instructions and actual scripts where applicable.

4.2 Conventions, SQL Server Nomenclature, and Directory Structure

In all cases throughout this chapter, when actual examples are provided, those which reference UNIX commands will be preceded by a “%”, and those that reference SQL statements will be preceded by a number and a “>” (e.g. 1>sp_help tablename).

The terms described in the following table will be used throughout the rest of this chapter.

Table 4.2-1. SQL Server General Definitions

Term	Definition
client	SYBASE Open Client software (version 10.0.2) located in the lib directory
Backup Server	Similar to the dataserver, it uses a separate UNIX process to off load the cycles associated with DUMP and LOAD commands
backups	The set of UNIX files containing full database dumps, transaction log dumps, and dbcc output
dbcc	Database Consistency Checker - a utility program designed to check
sybase root directory	/usr/ecs/Rel_A/COTS/sybase, this is the home directory for all SYBASE software and related products and is reference both in UNIX and in the rest of this document as \$SYBASE
interfaces file	Lists the names and access paths for all servers and backup servers that are part of the testbed.
sa	System Administrator login, this is the superuser of the SQL Server
scripts	UNIX script programs located in \$SYBASE/scripts and related subdirectories
showserver	A utility invoked at the UNIX command prompt to display active server, located in \$SYBASE/install .
SQL scripts	SQL and command statements located in \$SYBASE/scripts and related subdirectories
SQL	Structured Query Language

The **sybase** directory structure is described in the following table. Subdirectories under the **scripts** branch contain template files with easy to modify examples of SQL and SQL command syntax.

Table 4.2-2. SYBASE Directory Structure

Directory	Contains
\$SYBASE/bin	Utilities necessary to load, run, and access the server
\$SYBASE /install	Files used to start dataservers, backupserver and to record server messages (errorlogs)
\$SYBASE /lib	db-lib, ct-lib, and xa-lib client library files used by applications to gain access to the server
\$SYBASE /scripts	Root directory for all script files executed on the server
\$SYBASE /scripts/create.databases	SQL files used to create databases on the server
\$SYBASE /scripts/create.db_objects	SQL files used to create tables, indexes, triggers, rules, etc., in user databases
\$SYBASE /scripts/create.devices	SQL command files (disk init) used to map physical storage to a logical name
\$SYBASE /scripts/create.procedures	T-SQL file used to define stored procedure objects in user databases
\$SYBASE /scripts/create.users	SQL command files used to define logins and add them to user databases
backup directory	Root directory that contains all backup subdirectories, it is recommended, but not required, that this directory be on a separate physical disk
backup subdirectories	Created each evening by the RUN_backups cron job, they are named backups_for_YYMMDD and contain the following files: servername_dbname.dat - full database dumps servername_dbname_tx.dat - transaction file dumps (where applicable) servername_backup_log.YYMMDD servername_svr_stmts.out servername_svr_stmts.sql backup_summary.YYMMDD

Naming Conventions

As one of the most important, yet least applied concepts, naming conventions are presented in this chapter by examples according to the following rules.

Rule1: Regardless of the length of the name, it should indicate the function and/or content of the object

Rule 2: Only easily understandable abbreviations should be used

Rule 3: Parts of names are separated by underscores “_”, only one optional suffix is permitted (appended to the name by a “.”)

Rule 4: The full path of the object is considered to be part of the name

Notes and Examples:

The names of the databases and tables themselves may or may not follow the above rules, these rules are specifically for the DBA to work with SQL Server objects, and files in the UNIX environment.

All **COTS** software for the Pre-Release B Testbed is installed in the /usr/ecs/Rel_A/COTS directory.

All **SYBASE** software is located in the sybase root directory (**\$SYBASE**) or below.

The testbed has two SQL Servers installed, one for the Planning and Data Processing System (**pdps**) application, and one for autosys. The servers themselves are named MachineName_svr and autosys1_svr. In the case of the Goddard Testbed (where the name of the machine is **plng2sun**), the pdps application server is named **plng2sun_svr**. The names of all related files (e.g. Runserver, errorlog, etc.) have the Server Name incorporated in them.

All backups are located in directories below the Backup Directory, which may or may not be on a separate physical disk. The directories are kept for a period of 30 days and they are named as follows:

backups_for_YYMMDD

where YYMMDD is the “sortable” six digit year, month, and day. For example, on the date this chapter was written, a backup directory called backups_for_970423.

All sql script files have the extension **.sql** as a suffix. Their names reference the objects they create or functions they perform, and are all located either in **\$SYBASE/scripts** or below. For instance, an sql file to create the pdps_db_ops database is resident in **\$SYBASE/scripts/create.databases/pdps_db_ops.sql**, and another file used to alter the database might be called **\$SYBASE/scripts/create.databases/alter_pdps_db_ops.sql**.

4.3 SQL Server Installation

SYBASE SQL Server Version 10.0.2.6 has been installed and configured by the ECS Staff at Goddard Space Flight Center. Shared memory and disk resources have been allocated and configured by the System Administrator, and both the client and server portions have been set up by the DBA prior to shipment. The configuration of the system is described in the Pre-Release B Testbed Hardware/Software Mapping found in document 420-TD-006. The following table describes many of the parameters used and options chosen during installation.

Table 4.3-1. SQL Server Parameters and Options

Item	Brief Explanation
Server Name	plng2sun_srvr - GDAAC pdps application database server plng2sun_backup - Backup Server for the above dataserver autosys1_srvr - GDAAC autosys application database server autosys1_backup - Backup Server for the above dataserver
Port Numbers	The following standard number are used on all Testbed machine. Together with the Server Name information in the row above, these items describe the interfaces file resident on both server and all client machines in the \$SYBASE directory. 3021 - pdps application database server 3022 - pdps application Backup Server 3023 - autosys application database server 3024 - autosys application Backup Server
Release Directory	\$SYBASE
Retry Count	5
Retry Delay	5
master device	25 Mb raw partition
sybsemprocs	\$SYBASE/sybprocs.dat, 12 Mb and on it's own device
errorlog	\$SYBASE/install/plng2sun_srvr.errorlog
Current default language	us_english
Current default character set	iso_8859-1 (Latin-1)
Current sort order	Binary ordering, for the ISO 8859/1 or Latin-1 character set (iso_1).
Internal auditing	On
sybsecurity database size	175 Mb
sybsecurity device	sybsecuritydev, positioned on a 175 Mb raw partition

In the unlikely event that a server must be reinstalled, script files have been included from the previous installation that detail all DBA responses. The script files are located in the **\$SYBASE/install** directory. SQL Server installation is performed by an authorized user with the **sybinit** utility also located in the **\$SYBASE/install** directory. See your UNIX System Administrator and the SYBASE SQL Server Installation Guide.

4.4 DBA Functions

The following subsections detail the most common functions that a DBA will perform.

4.4.1 Starting, Stopping, and Showing the Server(s)

Use **shutdown** to bring the server to a halt. This command can only be issued by the System Administrator (sa).

Syntax: 1> **shutdown** [with nowait]
 2> go

The “with nowait” option shuts down the SQL Server immediately without waiting for currently executing statements to finish.

Use **startserver** to start an SQL Server and/or a Backup Server. This command can only be issued by the **sybase** user.

Syntax: % **startserver** [-f runserverfile]

The “runserverfile” is contained in the **\$SYBASE/install** directory.

Use **showserver** to determine whether the SQL Server(s) and/or Backup Server(s) are running.

Syntax: % **showserver**

Example output shows the UNIX processes running the various servers:

UID	PID	PPID	C	STIME	TTY	TIME	COMD
sybase	671	669	80	Apr 17	?	80:05	/usr/ecs/Rel_A/COTS/sybase/bin/dataserver -d /dev/rdisk/c1t0d0s1 -splng2sun_srvr
sybase	665	663	80	Apr 17	?	50:02	/usr/ecs/Rel_A/COTS/sybase/bin/backupserver -splng2sun_srvr -e/usr/ecs/Rel_A

4.4.2 Creating Logical Devices

A logical device is created when the UNIX System Administrator determines that new disk space is available for use by SYBASE software, databases, transaction logs, and/or backups. Either raw disk partitions or UNIX filesystem partitions can be used to create a logical device. The creation of a logical device is a mapping of physical space to a logical name and virtual device number (**vdevno**) contained in the SQL Server **master** database. The **DISK INIT** command is used to initialize this space. After the disk initialization is complete, the space described by the physical address is available to SQL Server for storage, and a row is added to the **sysdevices** table in the **master** database.

Example of Creating a Logical Device

A raw partition on a RAID device has been made available to SQL Server by the UNIX System Administrator. Essentially, the actual name of the raw device **c2t0d1s3** has had its ownership changed to **sybase** and its group changed to **user**.

- 1 In **\$SYBASE/scripts/create.devices**, DBA makes a script file from the template.

```
Syntax: % cd /usr/ecs/Rel_A/COTS/sybase/scripts/create.devices
        % cp template.sql data_dev1.sql
```

- 2 Appropriate items are modified so that the script file resembles the following:

DISK INIT

```
name = "data_dev1",
physname = "/dev/rdisk/c2t0d1s3",
vdevno = 3,
size = 128000
```

go

```
sp_helpdevice data_dev1
```

go

- 3 DBA runs the script from the UNIX command prompt:

```
Syntax:      % isql -Usa -Sservername -data_dev1.sql -odata_dev1.out
```

- 4 DBA checks the data_dev1.out file for success

4.4.3 Creating and Altering Databases

A user database is created by the DBA with a script containing the **CREATE DATABASE** command. A database is created on one or more physical devices. Specifying the device is optional - but highly recommended. When indicating the device, you use the logical name you specified as part of a DISK INIT (described above). Unlike the DISK INIT command, the size of the database data and log components is specified in MB instead of 2K pages.

Example of Creating a Database

The logical device **data_dev1** has been created (as above) along with another device called **tx_log1** (for transaction logging).

- 1 In **\$SYBASE/scripts/create.databases** directory, DBA makes a script file from the template.

```
Syntax: % cd /usr/ecs/Rel_A/COTS/sybase/scripts/create.databases
```

% cp template.sql userdb.sql

- 2 Appropriate items are modified so that the script file resembles the following:

```
create database UserDB on data_dev1 = 100 log on tx_log1 = 50
```

```
go
```

```
sp_helpdb UserDB
```

```
go
```

- 3 DBA runs the script from the UNIX command prompt:

Syntax: %isql -Usa -Sservername -iuserdb.sql -ouserdb.out

- 4 DBA checks the userdb.out file for success

Example of Altering a Database

The user database **UserDB** has run out of space and it has been determined that it should be increased by 50MB.

- 1 In **\$SYBASE/scripts/create.databases**, DBA creates a script file containing the **ALTER DATABASE** command (named **alter_userdb.sql**)

Syntax: Alter database UserDB on data_dev3 = 50

- 2 DBA runs the script from the UNIX command prompt:

Syntax: % isql -Usa -Sservername -ialter_userdb.sql -oalter_userdb.out

- 3 DBA checks the alter_userdb.out file for success

4.4.4 Data Placement - Segmentation

Segments are named subsets of the database devices available to a particular SQL Server database. Segment names are used in **CREATE TABLE** and **CREATE INDEX** commands to place tables or indexes on specific database devices. Using segments allows the DBA to better control the size of database objects and may improve performance by spreading i/o more evenly across devices.

Once the database device exists and is available, the segment can be defined with the system stored procedure **sp_addsegment**.

Syntax: sp_addsegment segname, dbname, devname

After the segment has been defined in the current database, the **CREATE TABLE** or **CREATE INDEX** commands use the optional clause "on segment_name" to place the object on a particular segment.

Syntax: CREATE TABLE table_name (column_name datatype ...) [on segment_name]

CREATE [clustered | nonclustered] INDEX index_name on table_name

Use **sp_helpdb** database_name after a **use** to display the segments defined for that database.

Use **sp_helpsegment** segment_name to list the objects on the segment and show the mapped devices.

Example of Creating a Segment

The DBA receives a request to create a segment for the storage of the DATA_INFO table indexes in the pdps_db_ops database, on a separate physical disk. Two devices **data_dev1** and **data_dev2** have already been created and are located on different physical disks.

1 In \$SYBASE/scripts/create.segments directory, DBA makes a script file from the template.

```
Syntax: % cd /usr/ecs/Rel_A/COTS/sybase/scripts/create.segments
        % cp template.sql segments_dev1.sql
```

2 The script file is modified so that it resembles the following:

```
sp_addsegment seg1_dev1, pdps_db_ops, data_dev1
sp_addsegment seg1_dev2, pdps_db_ops, data_dev2
go
```

3 DBA runs the script from the UNIX command prompt:

```
Syntax:      %isql -Usa -Sservername -ipdps_db_ops_segments.sql \
              -opdps_db_ops_segments.out
```

4 DBA checks the opdps_db_ops_segments.out file for success

5 When the table and indexes are created according to the instructions in section 4.4.6, the “on seg1_dev1” must be appended to the DATA_INFO.sql CREATE TABLE statement, and the “on seg1_dev2” must be appended to the DATA_INFO_indexes.sql CREATE INDEX statement.

Syntax: (example)

```
CREATE INDEX DATA_INFO_IDX on DATA_INFO (DI_ID) on SEG1_DEV2
```

4.4.5 Monitoring Space Usage

4.4.5.1 Thresholds

Thresholds are defined on segments to provide a free space value at which a procedure is executed to provide a warning or to take remedial action.

Use **sp_addthreshold** to define your own thresholds:

sp_addthreshold database_name, segment_name, free_space, procedure_name

where free_space is the number of free pages at which the threshold procedure executes; procedure_name is the stored procedure which the threshold manager executes when the number of free pages falls below the free_space value. Please see the section on Auditing later in this chapter for an example of Thresholds.

4.4.6 Creating Database Objects

In most, if not all cases, the database objects will be created by the database loading scripts furnished with the latest release of the testbed software. For special cases, creation (and modification) scripts are stored in **\$SYBASE**/scripts/create.db_objects. There should be a template for each type of object to be created.

Example of Creating a User Table

The DBA has received a request to authorize create a new table in the pdps_db_ops database called **PGE_Statistics** which has three column, pge_id, pge_statistic_type, and pge_statistic.

1 In the **\$SYBASE**/scripts/create.db_objects directory, DBA creates a script file from the proper template.

```
Syntax: % cd /usr/ecs/Rel_A/COTS/sybase/scripts/create.db_objects
        % cp table_template.sql PGE_Statistics_table.sql
```

2 Appropriate items are modified so that the script file resembles the following:

```
create table PGE_Statistics (
pge_id                int,
pge_statistic_type    int,
pge_statistic         float )
go
sp_help PGE_Statistic
go
```

3 DBA runs the script from the UNIX command prompt:

```
Syntax:      %isql -Usa -Sservername -iPGE_Statistics_table.sql \
              -oPGE_Statistics_table.out
```

4 DBA checks the PGE_Statistics_table.out file for success

Other objects are created in like manner but are not included here due to space considerations.

4.4.7 Creating and Managing Users Logins

In order to connect to a SQL Server a login must be created by the System Administrator or a system security officer. Login details are stored in the syslogins table in the **master** database.

The system stored procedure **sp_addlogin** adds new login names to the server but does not grant access to any user database.

Syntax: **sp_addlogin** login_name, password, [,default database ,language, fullname]

In order to gain access to a database, the System Administrator, system security officer, of the specific database owner must “add” the user with the **sp_adduser** system stored procedure.

Syntax: 1> **sp_adduser** jpublic, pdps_db_ops
 2> go

Example of Creating a Login and Granting Database Access

The DBA has received a request to authorize John Q. Public to the pdps_db_ops database.

1 In the **\$SYBASE/scripts/create.users** directory, DBA creates a script file containing the sp_addlogin command (named public.sql)

Syntax: % cd /usr/ecs/Rel_A/COTS/sybase/scripts/create.users
 % cp template.sql public.sql

2 DBA modifies appropriate fields so that the script resembles the following:

```
sp_addlogin jpublic,jpublic
go
use pdps_db_ops
go
sp_adduser jpublic
go
sp_helpuser
go
```

3 DBA runs the script from the UNIX command prompt:

Syntax: % isql -Usa -Sservername - public.sql -opublic.out

4 DBA checks the public.out file for success

4.4.8 Permissions

Permissions are used to control access within a database. The DBA uses the **GRANT** and **REVOKE** statements to accomplish this. There are two types of permissions within a database, **Object** and **Command**. In general, **Object** privileges control select, insert, update, delete, and execute permissions on tables, views, and stored procedures and **Command** permissions (which really do not apply to the Testbed) control access to the **CREATE** statements for databases, defaults, procedures, rules, tables, and views.

The syntax for the **GRANT** and **REVOKE** statements are quite similar:

```
GRANT {all [ privileges ] | command_list }  
to { public | name_list | role_name }
```

```
REVOKE {all [ privileges ] | command_list }  
from { public | name_list | role_name }
```

Example of Granting Privileges to a Specific User

The DBA receives a request that John Q. Public should be able to read the DATA_INFO table and read and update the SUBSCRIPTION_NOTIFICATION TABLE.

```
Syntax:      1> GRANT select on DATA_INFO to jpublic  
              2> GRANT all on SUBSCRIPTION_NOTIFICATION to jpublic  
              3> go
```

Note: It is recommended that the DBA store these command in a “.sql” file in the \$SYBASE/scripts/create.db_objects directory, along with their results.

4.5 Backup and Recovery

SQL Server backups are performed nightly by a **cron** job which runs the **RUN_backups** program located in the \$SYBASE/scripts/backups directory. The following table of definitions will be used throughout the rest of this section.

Table 4.5-1. Backup and Recovery Definitions

Term	Definition
Backup Script Components	Located in the \$\$SYBASE/scripts/backups directory, they include RUN_backups, backup.cron, make_backup_summary, make_backup_stmts.sql, and sp
Backup files	Defined in Table 4.2-2, the location of these files has been determined during server setup
Backup Statements	Generated from the sql in make_backup_stmts.sql these include calls to dbcc, Dump Database, and Dump Transaction commands
Backup Subdirectory	The only directory level underneath of the Backup Directory, defined in Table 4.2-2.
Backup Summary	An extraction of the successful Dump messages along with any errors generated by the Backup Statements stored in the Backup Subdirectory.

4.5.1 Automatic Backups

Full database and transaction log backups are performed nightly on the testbeds using the following Backup Script Components. All components are located in the **\$\$SYBASE/scripts/backups** directory.

Table 4.5-2. Automatic Backup Components

Component Name	Function(s)
backup.cron	File added with the crontab -e command, contains the following: 00 19 * * 1-6 /data1/COTS/sybase/scripts/backups/RUN_backups
RUN_backups	Controlling script that performs the following functions: create the Backup Subdirectory run isql to create the Backup Statements run isql to execute the Backup Statements record the results of the Backup Statements in Backup Files copy the Backup Files to the Backup Subdirectory create the Backup Summary
make_backup_stmts.sql	SQL statements that access the SQL Server master database (master..sysdatabases table) and create the Backup Statements
sp	SQL Server password file
make_backup_summary	UNIX shell script that “greps” successful Dump statements along with any errors generated and writes them to the backup_summary file

No intervention in the Automatic Backup Process is required by the DBA, though periodic checks of the Backup Subdirectories are recommended.

4.5.2 Manual Backups

Manual backups can be performed at any time by the System Administrator and are recommended for the following situations:

1. Any change to the **master** database - this includes new logins, devices, and databases
2. Any major change to user databases - a large ingest or deletion of data, definition of indexes
3. Other mission-critical activities - as defined by the DAAC Operations Controller

Both the **DUMP DATABASE** and **DUMP TRANSACTION** command processing are off-loaded to the backup server, and will not affect normal operations of the database. These commands are performed by the System Administrator on appropriate databases as follows:

Syntax: 1> dump database master to “/backup_directory/master.dat”

 2> go

- or in the case of a “standard” user database with a separate transaction log -

 1> dump database pdps_db_ops to “/backup_directory/pdps_db_ops.dat”

 2> go

 3> dump transaction pdps_db_ops to “/backup_directory/pdps_db_ops_tx.dat”

 4> go

4.5.3 Manual Recovery

Manual recovery of a user database is performed by the System Administrator by the use of the **LOAD DATABASE** and **LOAD TRANSACTION** commands. For issues concerning the **master** database, please consult your System Administrator’s Guide for assistance. It is recommended that any user database to be recovered be dropped and created with the **for load** option. In section 4.4.3, the **databasename.sql** along with any **alter.databasename.sql** scripts were saved, these need to be combined into one script which will re-create the user database with the **for load** option. This will insure the success of the **LOAD DATABASE** and **LOAD TRANSACTION** commands. The following example illustrates these issues:

4.5.4 The BulkCopy Utility

The **bcp** utility is located in the **\$SYBASE/bin** directory and is designed to copy data to and from SQL Server databases to operating system files.

4.5.4.1 Requirements for Using bcp

In general, you must supply the following information for transferring data to and from SQL Server:

- a. Name of the database and table

- b. Name of the operating system file
- c. Direction of the transfer (in or out)

In order to use **bcp**, you must have a SQL Server account and the appropriate permissions on the database tables and operating system files that you will use. To copy data **into** a table, you must have **insert** permission on that table. To copy data **out** to an operating system file, you must have select permission on the following tables:

- a. The table being copied
- b. sysobjects
- c. syscolumns
- d. sysindexes

4.5.4.2 bcp Syntax

```
bcp [[database_name].owner.]table_name {in | out} datafile [-e errfile] [-n] [-c]
    [-t field_terminator] [-r row_terminator] [-U username] [-P password] [-S server]
```

4.5.4.3 bcp Scripts and Files

The DAAC has developed two scripts: `bcp_out_testbed` and `bcp_in_testbed`. Use `bcp_out_testbed` as a template to copy data from a database and use `bcp_in_testbed` to copy data into a database.

Example of User Database Recovery

The database **UserDB** was created using the following script excerpt: (stored in `home/scripts/create.databases/userdb.sql`)

```
create database UserDB on data_dev1 = 100 log on tx_log1 = 50
```

and was modified using the following script excerpt: (`home/scripts/create.databases/alteruserdb.sql`)

```
Alter database UserDB on data_dev1=50
```

For the purposes of this example, the full database backup and transaction log dumps were successful and located in `home/backups/backups_for_970101/UserDB.dat` and `UserDB_tx.dat`

1 In the `$SYBASE/scripts/create.databases` directory, DBA makes a script file from the template.

```
Syntax: % cd /usr/ecs/Rel_A/COTS/sybase/scripts/create.databases
```

```
% cp template.sql userdb_for_load.sql
```

2 Appropriate items are modified so that the script file resembles the following:

```
create database UserDB on data_dev2=100 log on tx_log2=50 for load
```

```
go
```

```
Alter database UserDB on data_dev3=50
```

```
go
```

3 DBA saves the script in home/scripts/create.databases/ userdb_for_load.sql

4 DBA runs the script from the UNIX command prompt.

Syntax: %isql -Usa -S**servername** -iuserdb_for_load.sql -ouserdb_for_load.out

5 DBA checks the userdb_for_load.out file for success

6 DBA loads the database from the full backup.

Syntax: 1> LOAD DATABASE UserDB from

2> "home/backups/backups_for_970101/ UserDB.dat"

3> go

7 DBA loads the transaction file from the transaction file dump.

Syntax: 1> LOAD TRANSACTION UserDB from

2> "home/backups/backups_for_970101/ UserDB_tx.dat"

3>go

4.6 Database Performance and Tuning

Once your application is up and running, the DBA monitors its performance, and may want to customize and fine-tune it. Use the following software tools provided by SQL Server:

- a. Setting query processing options with the **set** command
- b. Setting database options with **sp_dboption**
- c. Monitoring SQL Server activity with **sp_monitor**
- d. Using **update statistics** to ensure that SQL Server makes the best use of existing indexes
- e. Changing system variables using **sp_configure** and the **reconfigure** command
- f. Placing objects on segments to spread i/o, improve throughput, etc. as described in section 4.4.4

For a complete discussion of issues related to SQL Server performance and tuning, refer to your SYBASE SQL Server System Administration Guide.

Table 4.7.1-1. Installation Steps for the pdps Application Database (2 of 2)

Step	Explanation
6. Load initial data	Run the load_activities.sql, load_dataserver_resource.sql, and loadmessages.sql edit the database name as before and execute them using the following example syntax: % isql -Usa -iload_activities.sql -oload_activities.out a. you will be prompted for the sa password b. check the out file carefully
7. Load initial autosys data	Edit trg_u_JOB.sql and change "exec MGD_SYBASE. pdps_phase3.." to "exec <sybase server>.<database name>". Edit trg_u_JOB_STATUS.sql and change "exec MGD_SYBASE. pdps_phase3.." to "exec <sybase server>.<database name>". Execute the script files using the following syntax: % isql -Usa -itrg_u_JOB.sql -otrg_u_JOB.out a. you will be prompted for the sa password b. check the out file carefully

4.7.2 The AUTOSYS Application and other Configuration Issues

The AUTOSYS application works in tandem with pdps to schedule the jobs that run on the Testbed Science Processor. Autosys installation is performed in /usr/ecs/Rel_A/COTS by the autosys_install program located in the autosys/bin directory. The Testbed should already have an installed and working copy of AUTOSYS, the results of the installation are stored in an autosys_install.scr file located in the AUTOSYS home directory (/use/ecs/Rel_A/COTS/autosys). For pdps to run properly with AUTOSYS, the following activities are completed:

- a. A user is defined to the Testbed SQL Server named **autosys**
- b. **autosys** user is added to the pdps_db_ops database
- c. The autosys server is added to the sysservers table on the Testbed server with **sp_addserver**
- d. The Testbed server is added to the sysservers table on the AUTOSYS server with **sp_addserver**

Further configuration and troubleshooting information is available from the ECS Staff at the Goddard Space Flight Center.

This page intentionally left blank.

5. Security Services

ECS security architecture must meet the requirements for data integrity, availability, and confidentiality. ECS Security Services meets these requirements by incorporating a variety of mechanisms to establish and verify user accounts, issue and verify passwords, audit user activity, and verify and protect data transfer. Security logs will be monitored and security reports generated by TO BE DETERMINED. Several COTS products provide tools for authentication and network and system monitoring: Kerberos, SATAN, Crack, npassword, TCP Wrapper, and Tripwire. The Open Software Foundation's Distributed Computing Environment (OSF/DCE) employs Kerberos for authenticating user requests for network services. (DCE administration tools are discussed in Section 3 of this document.) The COTS product, SATAN, monitors networks and finds system security vulnerabilities. Two COTS products — Crack and npassword — provide additional password protection for local system and network access. To monitor and control access to network services, ECS Security Services uses TCP Wrapper. The package, Tripwire, monitors changes to files and flags any unauthorized changes. Security Services also supports detection of, reporting, and recovery from security breaches. The products used for this tasking are TO BE DETERMINED.

This section defines step-by-step procedures for M&O personnel to run the Security Services tools. The procedures assume that the requester's application for a Security process has already been approved by DAAC Management. It is recommended that access to these tools be controlled through the **root access only**.

The Activity Checklist table that follows provides an overview of the Security process. Column one (**Order**) shows the order in which tasks are presented in this section. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 5-1. Security - Activity Checklist

Order	Role	Task	Section	Complete ?
1	Super User	Run Security Log Analyst Program	(P) 5.1	
2	Super User	Generate Security Reports	(P) 5.2	
3	Super User	Run Network Authentication Service	(P) 5.3	
4	Super User	Monitor Network Vulnerabilities	(P) 5.4	
5	Super User	Ensure Password Integrity	(P) 5.5	
6	Super User	Monitor Requests for Network Services	(P) 5.6	
7	Super User	Monitor File and Directory Integrity	(P) 5.7	
8	Super User	Report Security Breaches	(P) 5.8	
9	Super User	Initiate Recovery from Security Breaches	(P) 5.9	

5.1 Generating Security Reports

All COTS security products generate reports and log files. These are available when you run the product. Your System Administrator will be able to assist you.

5.2 Running the Network Authentication Service

Because intruders can monitor network traffic to intercept passwords, traditional authentication methods are not suitable for use in computer networks. The use of strong authentication methods that prevent password disclosure is essential. The Kerberos Network Authentication Service is well suited for such an environment.

Developed at the Massachusetts Institute of Technology, Kerberos is a distributed authentication service that allows a client (process that makes use of a network service) running on behalf of a principal (user or server) to identify itself to other principals, without sending data across the network that might allow an intruder to subsequently impersonate the user. Not knowing the identity of a user who requests an operation makes it difficult to decide whether the operation should be permitted.

The principal's level of permissions (such as read, create, modify, destroy) is based on DCE permissions and passwords established for the user. Kerberos reinforces DCE password security through its use of DES encryption (secret key) to protect sensitive information on an open network. In the case of a human user as the principal, the secret key is based on the user's password. However, the principal's password is **never** passed through the network.

Kerberos authentication activities are transparent to the user. Communication is between servers (principals) and processes (clients). The principal's request must receive a "ticket" that will be passed to each network service that the principal wants to access. The ticket is a record that helps a client authenticate itself to a server; it contains the client's identity, a session key, a timestamp, and other information, all sealed using the server's secret key. The session key is a temporary encryption key used between two principals, with a lifetime limited to the duration of a single login "session" (usually 8 hours).

Several utility programs must be installed on the user's workstation to allow users to obtain Kerberos credentials (kinit), list credentials (klist), and destroy credentials (kdestroy).

These procedures assume that the site is running MIT Kerberos 5, that the System Administrator has logged in as a super user, and that the Kerberos Authentication Server is available.

- 1 To login to the Kerberos Service, type **/bin/kinit** then press [RETURN].
Enter name and password.

- Acquires a ticket that is valid for the time of the session from the Kerberos authentication server. Once logged in, you will have access to the system as permitted by the tickets obtained from the Ticket Granting Service.

The following options can be used with the **kinit** command:

- f This option allows a ticket-granting ticket with a different network address than the present ticket-granting ticket's to be issued to the principal. For "forwarding" tickets to be granted, the principal's account in the registry must specify that the principal can be granted forwarding (or FORWARDABLE) tickets.
- v Specifies that the command should run in verbose mode.

2 At command line, type **klist** then press [RETURN].

- Acquires a list of tickets obtained for this session, for example:

Kerberos Ticket Information:

Ticket cache: /opt/dcelocal/var/security/creds/dcecred_031d6500

Default principal: reginald@edfcell.hitc.com

Server: krbtgt/edfcell.hitc.com@edfcell.hitc.com

valid 96/09/09:10:36:16 to 96/09/09:20:36:16

Server: dce-rgy@edfcell.hitc.com

valid 96/09/09:10:36:21 to 96/09/09:20:36:16

Server: dce-ptgt@edfcell.hitc.com

valid 96/09/09:10:36:25 to 96/09/09:12:36:25

Client: dce-ptgt@edfcell.hitc.com Server: krbtgt/edfcell.hitc.com@edfcell.

hitc.com

valid 96/09/09:10:36:25 to 96/09/09:12:36:25

Client: dce-ptgt@edfcell.hitc.com Server: dce-rgy@edfcell.hitc.com

valid 96/09/09:10:36:25 to 96/09/09:12:36:25

The following options can be used with the **klist** command:

- e Includes expired tickets in the display. Without this option, only current tickets are displayed.
- f Displays option settings on the tickets. The options are:
 - D** (postdatable)
 - dF** (postdated) (forwardable)

f (forwarded)

I (initial)

i (invalid)

P (proxiabale)

p (proxy)

R (renewable)

3 To logout of Kerberos Service, type **/bin/kdestroy** then press [RETURN].

- Destroys the ticket when the user logs out.

To share and mount files with Kerberos authentication:

4 Type **share -F nfs -o kerberos /filesystem** then press [RETURN].

- Shares a file system with Kerberos authentication.

5 Type **mount -F nfs -o kerberos server:resource mountpoint** then press [RETURN].

- Mounts a file system with Kerberos authentication.

6 To check the Kerberos Authentication Server, type **/Kerberos/Kerberos.log**.

5.3 Monitoring Network Vulnerabilities

The Security Administrator Tool for Analyzing Networks (SATAN) is a testing and reporting tool that collects a variety of information about networked hosts. SATAN gathers information about specified hosts and networks by examining network services (for example, finger, NFS, NIS, ftp). SATAN also gathers general network information (network topology, network services run, types of hardware and software being used on the network). The data is used to point out system vulnerabilities. Data can be reported in a summary format. Problems are described briefly and pointers provided to patches or workarounds.

Periodically, the operator will run SATAN as **root**. The procedures are provided below.

- 1** Make sure that **DISPLAY** is set on your workstation. **Note:** SATAN is run only on the SMC side (msss5hp).
- 2** From **/usr/ecs/Rel_A/COTS/secmgmt/satan-1.1.1** type **./satan**.
- 3** From the **SATAN Control Panel**, select **SATAN Configuration Management**. Set all variables or use the default values.

- 4 **Go back to the SATAN Control Panel.**
- 5 From the **SATAN Control Panel**, select **SATAN Data Management**. Create the SATAN database if it does not exist. When you create the database for the first time, you will see a warning message concerning password disclosures. Take no action and continue. The database is stored as **satan-data** in the directory **/satan-1.1.1/results**.
- 6 You will be notified when the SATAN finishes creating the database and scans the system (network or cluster) for vulnerabilities.
- 7 From this screen, you can click on "Continue with Reporting and Analysis" or you can return to the **SATAN Control Panel**, to make this selection. Select the reports that you want to review.

5.4 Ensuring Password Integrity

One aspect of system security is discretionary access control based on user passwords. Passwords should be so unique that they are virtually impenetrable to unauthorized users. Two COTS products provide utilities to create effective password practices. "Crack" detects weak passwords that could be easily bypassed, and "npasswd" enforces strong password rules.

Both of these products provide comprehensive dictionaries, which Crack and npasswd can shared. These "source" dictionaries provide lists of words, which if used, would create vulnerable passwords. You can add other dictionaries, for example, acronym lists, to eliminate commonly used terms from being used as passwords.

Crack and npasswd are installed in a secure location, that is, **root access only**. Such precautions are particularly apt when running Crack, which gives the administrator access to everyone's password that he/she penetrates.

5.4.1 Detecting Weak Passwords

Running Crack against a system's password file will enable a system administrator to assess how vulnerable the file is to unauthorized users and how well authorized users select secure passwords. Crack is designed to find standard Unix eight-character DES-encrypted passwords by standard guessing techniques.

Crack takes as its input a series of password files and source dictionaries. It merges the dictionaries, turns the password files into a sorted list, and generates lists of possible passwords from the merged dictionary or from information gleaned about users from the password file. It does not attempt to remedy the problem of allowing users to have guessable passwords, and it should NOT be used in place of getting a really good, secure password program replacement.

The instructions provided in the following sections are general in nature because how you configure Crack and how you run it depends on the platforms on which it resides and on the local

security requirements established for your site. M&O personnel should be familiar with these tasks to:

1. Configure the Crack shellscript and config.h files based on the README file and on requirements established for your site. See Section 5.4.1.1, below.
2. Run Crack based on requirements established for your site. See Section 5.4.1.2, below.
3. Customize the dictionaries. See Section 5.4.1.3, below.

5.4.1.1 Configuring Crack

Although Crack should already be configured for your system, the instructions are provided should you have to reconstruct the makefile as a result of file corruption. Crack has two configuration files: the Crack shellscript, which contains all the installation-specific configuration data, and the file Sources/conf.h, which contains configuration options specific to various binary platforms.

- 1 In the Crack shellscript, edit the `CRACK_HOME` variable to the correct value. This variable should be set to an absolute path name through which the directory containing Crack may be accessed on ALL machines on which Crack will be run. (Path names relative to username are acceptable as long as you have some sort of csh.)

There is a similar variable, `CRACK_OUT`, which specifies where Crack should put its output files — by default, this is the same as `$CRACK_HOME`.
- 2 Edit the file Sources/conf.h and establish which switches to enable. Each #define has a small note explaining its purpose. Portability of certain library functions, should not be a problem.
- 3 If using Crack -network (see Section 5.4.1.4, below), generate a Scripts/ **network.conf** file. This file contains a list of hostnames to rsh to, what their binary type is (useful when running a network Crack on several different architectures), an estimate of their relative power (take your slowest machine as unary, and measure all others relative to it), and a list of per-host flags to add to those specified on the Crack command line, when calling that host. There is an example of such a file provided in the Scripts directory.
- 4 To specify a more precise figure as to the relative power of your machines, play with the **command make** tests in the source code directory. This can provide you with the number of fcrypt()s that your machine can do per second, which is a number that you can plug into your **network.conf** as a measure of your machines' power (after rounding the value to an integer).

5.4.1.2 Running Crack

Crack is a self-installing program. Once the necessary configuration options for the Crack shellscrip and config.h have been set, the executables are created via **make** by running the Crack shellscrip.

Notes for Yellow Pages (NIS) Users:

To get Crack running from a YP password file, the simplest way is to generate a passwd format file by running:-

```
ypcat passwd > passwd.yp
```

and then running Crack on this file.

To launch Crack:

1 From **/usr/ecs/Rel_A/COTS/secmgmt/crack**, at the command line type: **./Crack**

2 For the single platform version:

```
./Crack [options] [bindir] /etc/passwd [...other passwd files]
```

3 For the network version:

```
./Crack -network [options] /etc/passwd [...other passwd files]
```

For a brief overview of the [options] available, see Section 5.4.1.4, below. Section 5.4.1.5 briefly describes several very useful scripts.

5.4.1.3 Creating Dictionaries

Crack works by making many individual passes over the password entries that you supply to it. Each pass generates password guesses based upon a sequence of rules, supplied to the program by the user. The rules are specified in a simplistic language in the files `gecos.rules` and `dicts.rules`, located in the Scripts directory (see Section 5.4.1.5, below).

Rules in Scripts/`gecos.rules` are applied to data generated by Crack from the `pw_gecos` and `pw_gecos` entries of the user's password entry. The entire set of rules in `gecos.rules` is applied to each of these words, which creates many more permutations and combinations, all of which are tested. After a pass has been made over the data based on `gecos` information, Crack makes further passes over the password data using successive rules from the Scripts/`dicts.rules` by loading the whole of Dicts/`bigdict` file into memory, with the rule being applied to each word from that file. This generates a resident dictionary, which is sorted and uniqued so as to prevent wasting time on repetition. After each pass is completed, the memory used by the resident dictionary is freed up, and re-used when the next dictionary is loaded.

Crack creates the Dicts/bigdict dictionary by merging, sorting, and uniq'ing the source dictionaries, which are to be found in the directory DictSrc and which may also be named in the Crack shellscript, via the \$STDDICT variable. (The default value of \$STDDICT is /usr/dict/words.)

The file DictSrc/bad_pws.dat is a dictionary which is meant to provide many of those common but non-dictionary passwords, such as 12345678 or qwerty.

To create your own dictionary:

- 1** Copy your dictionary into the DictSrc directory (use compress on it if you wish to save space; Crack will unpack it while generating the big dictionary).
- 2** Delete the contents of the Dicts directory by running Scripts/spotless. Your new dictionary will be merged in on the next run.

5.4.1.4 Options

-f Runs Crack in foreground mode, i.e., the password cracker is not backgrounded, and messages appear on stdout and stderr as you would expect. This option is only really useful for very small password files, or when you want to put a wrapper script around Crack.

Foreground mode is disabled if you try running Crack-network -f on the command line, because of the insensibility of rshing to several machines in turn, waiting for each one to finish before calling the next. For more information, read the section about Network Cracking without NFS/RFS in the README.NETWORK file.

-v Sets verbose mode, whereby Crack will print every guess it is trying on a per-user basis. This is a very quick way of flooding your filestore, but useful if you think something is going wrong.

-m Sends mail to any user whose password you crack by invoking Scripts/nastygram with their username as an argument. The reason for using the script is so that a degree of flexibility in the format of the mail message is supplied; i.e., you don't have to recompile code in order to change the message.

-nvalue Sets the process to be nice()ed to value, so, for example, the switch -n19 sets the Crack process to run at the lowest priority.

-network Throws Crack into network mode, in which it reads the Scripts/network.conf file, splits its input into chunks which are sized according to the power of the target machine, and calls rsh to run Crack on that machine. Options for Crack running on the target machine may be supplied on the command line (for example, verbose or recover mode), or in the network.conf file if they pertain to specific hosts (e.g., nice() values).

-r<pointfile>

This is only for use when running in recover mode. When a running Crack starts pass 2, it periodically saves its state in a pointfile, with a name of the form Runtime/P.* This file can be used to recover where you were should a host crash. Simply invoke Crack in exactly the same manner as the last time, with the addition of the **-r** switch (for example, **-rRuntime/Pfred12345**). Crack will startup and read the file, and jump to roughly where it left off. If you are cracking a very large password file, this can save a lot of time after a crash.

5.4.1.5 Crack Support Scripts

The Scripts directory contains a small number of support and utility scripts, some of which are designed to help Crack users check their progress. The most useful scripts are briefly described below.

Scripts/shadmrq

This is a small script for merging /etc/passwd and /etc/shadow on System V style shadow password systems. It produces the merged data to stdout, and will need redirecting into a file before Crack can work on it.

Scripts/plaster

This is a simple frontend to the Runtime/D* diefiles that each copy of the password cracker generates. Invoking Scripts/plaster will kill off all copies of the password cracker you are running, over the network or otherwise. Diefiles contain debugging information about the job, and are generated so that all the jobs on the entire network can be called quickly by invoking Scripts/plaster. Diefiles delete themselves after they have been run.

Scripts/status

This script rshes to each machine mentioned in the Scripts/network.conf file, and provides some information about processes and uptime on that machine. This is useful when you want to find out just how well your password crackers are getting on during a Crack -network.

Scripts/{clean,spotless}

These are really just frontends to a makefile. Invoking Scripts/clean tidies up the Crack home directory, and removes probably unwanted files, but leaves the pre-processed dictionary bigdict intact. Scripts/spotless does the same as Scripts/clean but obliterates bigdict and old output files, too, and compresses the feedback files into one.

Scripts/nastygram

This is the shellscript that is invoked by the password cracker to send mail to users who have guessable passwords, if the **-m** option is used. Edit it to suit your system.

Scripts/guess2fbk

This script takes your out* files as arguments and reformats the 'Guessed' lines into a slightly messy feedback file, suitable for storing with the others.

An occasion where this might be useful is when your cracker has guessed many peoples' passwords, and then died for some reason (a crash?) before writing out the guesses to a feedback file. Running `Scripts/guess2fbk out* >> Runtime/F.new` will save the work that has been done.

5.4.1.6 Checking the Log

Crack loads dictionaries directly into memory, sorts and uniques them, before attempting to use each of the words as a guess for each users' password. If Crack correctly guesses a password, it marks the user as done and does not waste further time on trying to break that user's password.

Once Crack has finished a dictionary pass, it sweeps the list of users looking for the passwords it has cracked. It stores the cracked passwords in both plain text and encrypted forms in a feedback file in the directory **Runtime**. Feedback files have names of the form **Runtime/F***. The purpose of this is so that when it is next invoked, Crack can recognize passwords that it has successfully cracked previously, and filter them from the input to the password cracker. This provides an instant list of crackable users who have not changed their passwords since the last time Crack was run. This list appears in a file with name **out*** in the **\$CRACK_OUT** directory, or on **stdout**, if foreground mode (**-f**) is invoked (see Section 5.4.1.4, above).

Similarly, when a Crack run terminates normally, it writes out to the feedback file all encrypted passwords that it has NOT succeeded in cracking. Crack will then ignore all of these passwords next time you run it.

Obviously, this is not desirable if you frequently change your dictionaries or rules, and so there is a script provided, **Scripts/mrgfbk**, which sorts your feedback files, merges them into one, and optionally removes all traces of "uncrackable" passwords, so that your next Crack run can have a go at passwords it has not succeeded in breaking before.

mrgfbk is invoked automatically if you run **Scripts/spotless** (see Section 5.4.1.5, above).

5.4.2 Enforcing Strong Passwords

"npasswd" is a "drop-in" replacement for the normal Unix "passwd" command, which is transparent to the user. npasswd performs some simple length and character type tests on a proposed password and then checks it against the words in the dictionaries and rules specified in the configuration file. When the user changes his/her password (or inputs one for the first time), npasswd will check the password against the dictionaries and the rules. If it passes the check, the password is accepted. If the password fails, npasswd provides a message to the user, explains why the password fails, and asks the user to try again.

5.4.2.1 Configuring npasswd

Configure npasswd to establish the password rules for your site:

- 1 Edit the makefile, '**npasswd.conf**'. Choose the version of npasswd you want to be the default (based on the platform on which npasswd will reside) and retarget '**all**' in the Makefile to point to it. For example,
 - For running under **SunOS 4.X** system, set **OPTIONS = -DSUNOS4**. If you are thinking about running Sun "Secure RPC," add **DSECURE_RPC** to **OPTIONS**
 - For running under **System V**, set **OPTIONS = -DSYSV**
 - To use syslog(3), include **-DSYSLOG** in **OPTIONS**
 - To update the 4.3BSD hashed password database, include '**-DBSD4_3**' in **OPTIONS**.
 - Change the lines for 'CF' and 'HF' to retarget the config and or help files.

- 2 Continue to edit '**npasswd.conf**' to reflect your preferences. We recommend the following values:

# dictionary	/path/to/dictionary	Description
# dictionary	/usr/dict/words	Standard word list
# dictionary	/usr/dict/new_words	Additional word list
# dictionary	/etc/local_words	Local names to avoid

Note: npasswd can use the same dictionaries as Crack.

Don't allow single-case passwords

singlecase no

Minimum password length

minlength 8

Maximum effective password length

maxlength

(warns that you have exceeded the maximum number of characters. If you type in 10 characters and the maxlength is 6, npasswd will accept the first 6 characters you type in.)

#Don't forbid unprintable characters

printonly yes

Disallow the '@' character because of its incompatibility with HP/UX. See "Replace illegal character list," below. (**Note:** Disallow "@" even if you are not working on an HP/UX.)

Replace illegal character list

badchars "<string>" For example: badchars "@"

Set a list of characters forbidden in passwords.

This form REPLACES the built-in illegal character list (see below).

Control characters may be specified by the '^X' convention.

Add to illegal character list

badchars +"<string>"

Adds to the built-in illegal character list. Uncomment if you want to use it.

- 3 Edit '**npasswd.help**' to reflect the preferences chosen for the password checking plus add any other local administrative details.

5.4.2.2 **Building npasswd**

These instructions are provided should you have to rebuild npasswd because of file corruption.

- 1 Do a '**make**' to build the executables.
- 2 Become super-user and do '**make install**'.
- 3 If you built npasswd with **-DSYSLOG**, modify **/etc/syslog.conf** to log messages for facility **LOG_AUTH** level **LOG_INFO**. This gives you a record of password changes.

5.5 **Monitoring Requests for Network Services**

With TCP Wrapper, you can monitor and filter incoming requests for network services, such as SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, EXEC, TFTP, and TALK.

TCP Wrapper provides small daemon wrapper programs that can be installed without any changes to existing software or to existing configuration files. The wrappers report the name of the client host and the name of the requested service; the wrappers do not exchange information with the client or server applications, and impose no overhead on the actual conversation

between the client and server applications. The usual approach is to run one single daemon process that waits for all kinds of incoming network connections. Whenever a connection is established, this daemon runs the appropriate server program and goes back to sleep, waiting for other connections.

M&O personnel will monitor requests for these network services:

Client	Server	Application
telnet	telnetd	remote login
ftp	ftpd	file transfer
finger	fingerd	show users
rlogin	rlogind	remote login
TFTP	TFTPD	Trivial FTP

You will monitor the **syslog** file. To view syslog, at the command line type

```
more/var/log/syslog
```

Standard Unix commands can be added, such as vi, emacs, or lp -d:

```
more/var/log/syslog | lp -d [printer name]
```

The syslog file provides information concerning who tried to access the network service. TCP Wrapper blocks any request made by unauthorized users. TCP Wrapper can be configured to send a message to any administrator whose request is rejected.

5.6 Monitoring File and Directory Integrity

Tripwire is a tool that aids in the detection of unauthorized modification of files resident on Unix systems. Tripwire is automatically invoked at system startup. This utility checks file and directory integrity by comparing a designated set of files and directories against information stored in a previously generated database. Tripwire flags and logs any differences, including added or deleted entries. When run against system files regularly, Tripwire spots any changes in critical system files, records these changes into its database, and notifies system administrators of corrupted or tampered files so that they can take damage control measures quickly and effectively. With Tripwire, system administrators can conclude with a high degree of certainty that a given set of files remain free of unauthorized modifications if Tripwire reports no changes.

Note: Since system files should not change and users' files change constantly, Tripwire should be used to **monitor only system files**. The list of system files you want to monitor is stored in **./configs/tw.conf**. See Section 5.6.2, below.

Tripwire is configured to mail the system administrator any output that it generates. However, some files on your system may change during normal operation, and this necessitates updating the Tripwire database.

5.6.1 Updating the Tripwire Database

You can update your Tripwire database in two ways. The first method is interactive, where Tripwire prompts the user whether each changed entry should be updated to reflect the current state of the file, while the second method is a command-line driven mode where specific files/entries are specified at run-time.

5.6.1.1 Updating Tripwire Database in Interactive mode

Running Tripwire in Interactive mode is similar to the Integrity Checking mode. However, when a file or directory is encountered that has been added, deleted, or changed from what was recorded in the database, Tripwire asks the user whether the database entry should be updated.

For example, if Tripwire is run in Interactive mode and a file's timestamp changed, Tripwire will print out what it expected the file to look like, what it actually found, and then prompt the user whether the file should be updated. For example,

```
/etc/hosts equiv
      st_mtime: Wed May  5 15:30:37 1993      Wed May  5 15:24:09 1993
      st_ctime: Wed May  5 15:30:37 1993      Wed May  5 15:24:09 1993
---> File: /etc/hosts equiv
---> Update entry? [YN(y)nh?] y
```

You could answer yes or no, where a capital 'Y' or 'N' tells Tripwire use your answer for the rest of the files. (The 'h' and '?' choices give you help and descriptions of the various inode fields.)

While this mode may be the most convenient way of keeping your database up-to-date, it requires that the user be "at the keyboard." A more conventional command-line driven interface exists, and is described next.

5.6.1.2 Updating Tripwire Database in Database Update Mode

Tripwire supports incremental updates of its database on a per-file/directory or tw.config entry basis. Tripwire stores information in the database so it can associate any file in the database with the tw.config entry that generated it when the database was created.

Therefore, if a single file has changed, you can:

```
tripwire -update /etc/newly.installed.file
```

Or, if an entire set of files that made up an entry in the tw.config file changed, you can:

```
tripwire -update /usr/local/bin/Local_Package_Dir
```

In either case, Tripwire regenerates the database entries for every specified file. A backup of the old database is created in the **./databases** directory.

Tripwire can handle arbitrary numbers of arguments in Database Update mode.

The script **twdb_check.pl** script is an interim mechanism to ensure database consistency. Namely, when new entries are added to the **tw.config** file, database entries may no longer be associated with the proper entry number. The **twdb_check.pl** script analyzes the database, and remaps each database entry with its proper **tw.config** entry.

5.6.2 Configuring the **tw.config** file

Edit your **tw.config** file in the **./configs** directory, or whatever filename you defined for the Tripwire configuration file, and add all the directories that contain files that you want monitored. The format of the configuration file is described in its header and in the "man" page. Pay especially close attention to the **select-flags** and **omit-lists**, which can significantly reduce the amount of uninteresting output generated by Tripwire. For example, you will probably want to omit files like mount tables that are constantly changed by the operating system.

Run Tripwire with **tripwire -initialize**. This will create a file called **tw.db_[hostname]** in the directory you specified to hold your databases (where [hostname] will be replaced with your machine hostname).

Tripwire will detect changes made to files from this point on. You ***must*** be certain that the system on which you generate the initial database is clean; however, Tripwire cannot detect unauthorized modifications that have already been made. One way to do this would be to take the machine to single-user mode, reinstall all system binaries, and run Tripwire in initialization mode before returning to multi-user operation.

This database must be moved someplace where it cannot be modified. Because data from Tripwire is only as trustworthy as its database, choose this with care. It is recommended to place all the system databases on a read-only disk (you need to be able to change the disk to writeable during initialization and updates, however), or exporting it via read-only NFS from a "secure-server." (This pathname is hardcoded into Tripwire. Any time you change the pathname to the database repository, you must recompile Tripwire. This prevents a malicious intruder from spoofing Tripwire into giving a false "okay" message.)

We also recommend that you make a hardcopy printout of the database contents right away. In the event that you become suspicious of the integrity of the database, you will be able to manually compare information against this hardcopy.

Once you have your database set up, you can run Tripwire in Integrity Checking mode by typing **tripwire** on the command line from the directory in which Tripwire has been installed.

5.7 Reporting Security Breaches

TO BE SUPPLIED.

5.8 Initiating Recovery from Security Breaches

TO BE SUPPLIED.

This page intentionally left blank.

6. Network Administration

6.1 HP Open View Network Node Manager (NNM)

HP Open View Network Node Manager (NNM) is a multivendor network management application for use in managing TCP/IP networks and network devices that support the Simple Network Management Protocol (SNMP). NNM is an HP Open View SNMP-based application running under the HP Open View Windows (OVW) graphical user interface.

The NNM product is a configuration, performance, and fault management application for multivendor TCP/IP (Transmission Control Protocol/Internet Protocol) networks. NNM enables you to:

Automatically discover the devices on the TCP/IP network and monitor the status of those devices.

Automatically draw the Internet Protocol (IP) topology maps based on discovered information. A map is a graphical and hierarchical representation of your network and its systems. Discovered devices are placed in appropriate segments, networks, or Internet based on the topology of the IP network.

Manage any vendor devices that support the Simple Network Management Protocol (SNMP). NNM can manage standard MIB objects, as well as Enterprise-specific Management Information Base (MIB) objects.

Include new Enterprise-specific MIBs into the NNM MIB. Once you have loaded the new MIB module on the management station, you can manage any of the MIB objects defined in that MIB module.

The Activity Checklist table that follows provides an basic overview of the NNM functions. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number of Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 6.1-1. Network Administration - Activity Checklist

Order	Role	Task	Section	Complete?
1	Net Admin.	Start Network Node Manager	(P) 6.1.1	
2	Net Admin.	Add a Network Object	(P) 6.1.2.1	
3	Net Admin.	Add a Segment Object	(P) 6.1.2.2	
4	Net Admin.	Add a Node Object	(P) 6.1.2.3	
5	Net Admin.	Add an IP Interface Object	(P) 6.1.2.4	
6	Net Admin.	View the Current Network and System Configuration	(P) 6.1.3	
7	Net Admin.	View Network Address Information	(P) 6.1.4	
8	Net Admin.	View How Traffic is Routed on a Network	(P) 6.1.5	
9	Net Admin.	View the Services Available on a Node	(P) 6.1.6	

Detail procedures for tasks performed by the Network Administrator are provided in the sections that follow. The procedures assume that the administrator is authorized and has proper access privileges to perform the tasks.

6.1.1 Starting Network Node Manager (NNM)

HP Open View Network Node Manager is a set of applications that are integrated with HP Open View Windows (OVW). To Start NNM, HP OpenView Windows must be activated first. Once activated, OVW will automatically start NNM. HP OpenView windows will also automatically start the applications that are installed and registered.

Table 6.1-2 presents the procedures to start NNM in a condensed manner for quick reference. If you are already familiar with the procedures, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

Prerequisites for this Task

The network management processes that work with OVW and NNM must be running. The network management processes consist of the following HP OpenView background processes: **ovwdb**, **trapd**, **ovtopmd**, **ovactiond**, **snmpCollect**, and **netmon**. You can check to see if these processes are running with **/usr/ov/bin/ovstatus** command.

These procedures explain how to start the HP OpenView Windows graphical user interface:

- 1 Type **ovstart** at the command prompt and **press Enter**.
 - If the network management processes are not running, you can start them by executing the **\$OV_BIN/ovstart** command.
- 2 Type **ovstatus** at the command prompt and **press Enter**.

- This command will check the status of the processes.
- 3** Type **x11start** at the command prompt and **press Enter**.
 - This command will start the X Windows session.
- 4** Type **ovw** at the command prompt and **press Enter**.
 - The **\$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
 - If the **\$OV_BIN** directory is not in your path, type **\$OV_BIN/ovw** to start HP OpenView Windows.

To exit NNM and all other integrated applications, you must exit OVW. You can exit OVW in **one** of the following ways:

- 5** Select **File: Exit** from the menu bar of any submap window or go to step number 6;
- 6** **Click** on the **Close** button on all open submap windows until a black submap window is displayed. When the black submap window is displayed, click on the **Close** button.
 - The open map is saved, and all the submap windows and dialog boxes of the map are closed. OVW, all NNM applications, and all other integrated applications are closed.

Table 6.1-2. Starting NNM (Network Node Manager) - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	ovstart \$OV_BIN/ovstart if network management processes are not running	press Enter
2	ovstatus	press Enter
3	x11start	press Enter
4	ovw \$OV_BIN/ovw if \$OV_BIN directory is not in the path	press Enter
	<i>To exit Network Node Manager: (2 methods)</i>	
5	Exit	File → Exit
6	Close button on all open submap windows	single-click on Close button

6.1.2 Creating Additional Objects

To complete the distribution of resources over the map to better match how your network is organized, you must first expand the lower levels of the network map by creating additional network, segment, and node objects. The following sections show how to add network, segment, node, and interface objects to the network map so that IP Map will manage them.

6.1.2.1 Adding a Network Object

Table 6.1-3 presents the procedures to add a network object to the network map in a condensed manner for quick reference. If you are already familiar with the procedures, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

Prerequisites for this Task

The map must be opened with read-write access.

- 1** Type **ovstart** at the command prompt and **press Enter**.
 - If the network management processes are not running, you can start them by executing the **\$OV_BIN/ovstart** command.
- 2** Type **ovstatus** at the command prompt and **press Enter**.
 - This command will check the status of the processes.
- 3** Type **x11start** at the command prompt and **press Enter**.
 - This command will start the X Windows session.
- 4** Type **ovw** at the command prompt and **press Enter**.
 - The **\$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
 - If the **\$OV_BIN** directory is not in your path, type **\$OV_BIN/ovw** to start HP OpenView Windows.
- 5** Select **Edit: Add object**
- 6** From the **symbol palette**, choose the desired symbol type for the network object by **selecting the desired subclass and use button 2 to drag the symbol to the submap**. The **Add object** dialog box appears.
- 7** Enter a selection name for the object in the **Selection Name** field of the **Add Object** dialog box.
- 8** In the **Object Attributes** list, select **IP Map** and click **Set Object Attributes**. The **IP Map Set Attributes** dialog box for a network object appears.
- 9** Enter a **Network Name**.
- 10** Enter a **Network Address**.
- 11** Optionally, **Network Subnet Mask** can be entered.
- 12** Click **Verify** to check for valid entries.
- 13** Click on **OK** to close the **Set Attributes** dialog box.

- 14 Click on **OK** in the **Add Object** dialog box to complete the operation.

Table 6.1-3. Adding a Network Object - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	ovstart \$OV_BIN/ovstart if network management processes are not running	press Enter
2	ovstatus	press Enter
3	x11start	press Enter
4	ovw \$OV_BIN/ovw if \$OV_BIN directory is not in the path	press Enter
5	Edit:	select with mouse
6	Select the desired symbol type	select with mouse
7	Selection Name	(No action)
8	Select IP Map	click Set Object Attributes
9	Enter Network Name	press Enter
10	Enter Network Address	press Enter
11	Enter Network Subnet Mask (Optional)	press Enter
12	Select Verify	select with mouse
13	Select OK to close the Set Attributes	select with mouse
14	Select OK in the Add Object	select with mouse

6.1.2.2 Adding a Segment Object

If it can identify which segment the node is on, IP Map places the segment on that node. If it cannot make the identification, IP Map places the segment on the default segment submap. The default segment submap is the submap created by IP Map when OVW was first started. If that submap has been deleted, the default segment submap becomes the oldest segment submap. IP Map discovers new nodes on segments attached to SNMP, IP addressable bridges and multi-port repeaters (hubs).

Table 6.1-4 presents the procedures to add a segment object to the network map in a condensed manner for quick reference. If you are already familiar with the procedures, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

Prerequisites for this Task

The map must be opened with read-write access.

- 1 Type **ovstart** at the command prompt and **press Enter**.
 - If the network management processes are not running, you can start them by executing the **\$OV_BIN/ovstart** command.
- 2 Type **ovstatus** at the command prompt and **press Enter**.

- This command will check the status of the processes.
- 3** Type **x11start** at the command prompt and **press Enter**.
 - This command will start the X Windows session.
- 4** Type **ovw** at the command prompt and **press Enter**.
 - The **\$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
 - If the **\$OV_BIN** directory is not in your path, type **\$OV_BIN/ovw** to start HP OpenView Windows.
- 5** Select **Edit: Add Object**.
- 6** From the **symbol palette**, choose the desired symbol type for the segment object by selecting the desired class, then the desired subclass, and drag the symbol to the submap. The **Add Object** dialog box appears.
- 7** Enter a selection name for the object in the **Selection Name** field of the **Add Object** dialog box.
- 8** In the **Object Attributes** list, select **IP Map** and click **Set Object Attributes**. The **IP Map Set Attributes** dialog box for a segment object appears. A figure of the dialog box follows this procedure.
- 9** Enter a **name for the segment**. It must be unique to other segment names in the submap.
- 10** Click **Verify** to check for valid entries.
- 11** Click on **OK** to close the **Set Attributes** dialog box.
- 12** Click on **OK** in the **Add Object** dialog box to complete the operation.

Table 6.1-4. Adding a Segment Object- Quick-Step Procedures (1 of 2)

Step	What to Enter or Select	Action to Take
1	ovstart \$OV_BIN/ovstart if network management processes are not running	press Enter
2	ovstatus	press Enter
3	x11start	press Enter
4	ovw \$OV_BIN/ovw if \$OV_BIN directory is not in the path	press Enter
5	Select Edit: Add Object	select with mouse
6	Desired symbol type for the segment object by	select desired class, then the desired subclass, and drag the symbol to the submap
7	Enter Selection Name	press Enter
8	Select IP Map	click on Set Object Attributes

Table 6.1-4. Adding a Segment Object- Quick-Step Procedures (1 of 2)

Step	What to Enter or Select	Action to Take
9	Enter a name for the segment (must be unique)	press Enter
10	Select Verify	select with mouse
11	Select OK to close the Set Attributes	select with mouse
12	Select OK in the Add Object dialog box	select with mouse

6.1.2.3 Adding a Node Object

An Object can be added that represents a node or a network device to Segment submap by placing one of the supported symbols on a Segment submap. Double-clicking on the node symbol opens a Node submap. IP Map discovers and manages the symbols that represent the Computer, Connector, and Net Device classes in a Node submap.

Table 6.1-5 presents the procedures to add a node object to the network map in a condensed manner for quick reference. If you are already familiar with the procedures, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

Prerequisites for this Task

The map must be opened with read-write access.

- 1 Type **ovstart** at the command prompt and **press Enter**.
 - If the network management processes are not running, you can start them by executing the **\$OV_BIN/ovstart** command.
- 2 Type **ovstatus** at the command prompt and **press Enter**.
 - This command will check the status of the processes.
- 3 Type **x11start** at the command prompt and **press Enter**.
 - This command will start the X Windows session.
- 4 Type **ovw** at the command prompt and **press Enter**.
 - The **\$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
 - If the **\$OV_BIN** directory is not in your path, type **\$OV_BIN/ovw** to start HP OpenView Windows.
- 5 Select **Edit: Add Object**
- 6 From the **symbol palette**, choose the desired symbol type for the node object by selecting the desired class, then the desired subclass, and drag the symbol to the submap. The Add Object dialog box appears.
- 7 Enter a selection name for the object in the **Selection Name** field of the **Add Object** dialog box.

- 8 In the **Object Attributes** list, select **IP Map**, and click **Set Object Attributes**. The **IP Map Set Attributes** dialog box for a node object appears.
- 9 Enter the hostname of the node.
- 10 Enter the IP address of the node.
- 11 Click **Verify** to check for valid entries.
- 12 Click on **OK** to close the **Set Attributes** dialog box.
- 13 Click on **OK** in the **Add Object** dialog box to complete the operation.

Table 6.1-5. Adding a Node Object- Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	ovstart \$OV_BIN/ovstart if network management processes are not running	press Enter
2	ovstatus	press Enter
3	x11start	press Enter
4	ovw \$OV_BIN/ovw if \$OV_BIN directory is not in the path	press Enter
5	Select Edit: Add Object	select with mouse
6	Desired symbol type for the segment object	select desired class, then the desired subclass, and drag the symbol to the submap
7	Enter selection name	press Enter
8	Select IP Map	click Set Object Attributes
9	Enter hostname of the node	press Enter
10	Enter the IP address of the node	press Enter
11	Select Verify	select with mouse
12	Select OK to close the Set Attributes	select with mouse
13	Select OK in the Add Object to complete the operation	select with mouse

6.1.2.4 Adding an IP Interface Object

IP interface can be added to a Node submap by placing an IP Interface symbol on a Node submap. This is done by entering the IP address of the interface.

Table 6.1-6 presents the procedures to add an IP interface object to the network map in a condensed manner for quick reference. If you are already familiar with the procedures, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

Prerequisites for this Task

The map must be opened with read-write access.

- 1** Type **ovstart** at the command prompt and **press Enter**.
 - If the network management processes are not running, you can start them by executing the **\$OV_BIN/ovstart** command.
- 2** Type **ovstatus** at the command prompt and **press Enter**.
 - This command will check the status of the processes.
- 3** Type **x11start** at the command prompt and **press Enter**.
 - This command will start the X Windows session.
- 4** Type **ovw** at the command prompt and **press Enter**.
 - The **\$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
 - If the **\$OV_BIN** directory is not in your path, type **\$OV_BIN/ovw** to start HP OpenView Windows.
- 5** Select **Edit: Add Object**.
- 6** From the **symbol palette**, select the **IP Interface** symbol in the **Cards** class. The Add Object dialog box appears.
- 7** Enter a **selection name for the object** in the **Selection Name** field of the **Add Object dialog box**.
- 8** In the Object Attributes list, **select IP Map**, and click **Set Object Attributes**. The IP Map Set Attributes dialog box for an IP Interface object appears.
- 9** Enter the **IP Address for the IP interface**. The subnet mask is added for you.
- 10** Click **Verify** to check for valid entries.
- 11** Click on **OK** to close the Set Attributes dialog box.
- 12** Click on **OK** in the Add Object dialog box to complete the operation.

Table 6.1-6. Adding an IP Interface Object- Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	ovstart \$OV_BIN/ovstart if network management processes are not running	press Enter
2	ovstatus	press Enter
3	x11start	press Enter
4	ovw \$OV_BIN/ovw if \$OV_BIN directory is not in the path	press Enter
5	Select Edit: Add Object	select with mouse
6	Select the IP Interface	select with mouse
7	Enter selection name for the object	press Enter
8	Select IP Map	select Set Object Attributes
9	Enter IP Address for the IP interface	press Enter
10	Select Verify	select with mouse
11	Select OK to close the Set Attributes dialog box	select with mouse
12	Select OK in the Add Object dialog box	select with mouse

6.1.3 Viewing the Current Network and System Configuration

NNM provides quick access to information about your network and system configurations. This section points you to the menu items available to accessing this information.

Table 6.1-7 presents the procedures to view the current network and system configuration in a condensed manner for quick reference. If you are already familiar with the procedures, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

Prerequisites for this Task

One or more nodes must be selected from the map. If you select more than one node, you receive a dialog box for each selected node.

- 1 Type **ovstart** at the command prompt and **press Enter**.
 - If the network management processes are not running, you can start them by executing the **\$OV_BIN/ovstart** command.
- 2 Type **ovstatus** at the command prompt and **press Enter**.
 - This command will check the status of the processes.
- 3 Type **x11start** at the command prompt and **press Enter**.
 - This command will start the X Windows session.
- 4 Type **ovw** at the command prompt and **press Enter**.

- The **\$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
 - If the **\$OV_BIN** directory is not in your path, type **\$OV_BIN/ovw** to start HP OpenView Windows.
- 5 Select the **object** for which you want a description.
 - 6 Select Monitor: **Description - Selected Objects**. The **Object Description** dialog box appears.
 - 7 In the **Object Description** dialog box, select **IP Map** and select **View/Modify Object Attributes**. The **Set Attributes** dialog box appears.

Table 6.1-7. Viewing the Current Network and System Configuration - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	ovstart \$OV_BIN/ovstart if network management processes are not running	press Enter
2	ovstatus	press Enter
3	x11start	press Enter
4	ovw \$OV_BIN/ovw if \$OV_BIN directory is not in the path	press Enter
5	Select the object for which you want a description	select with mouse
6	Select Monitor: Description - Selected Object	select with mouse
7	Select IP Map	Select with mouse
7	Select View/Modify Object Attributes	Select with mouse

6.1.4 Viewing Network Address Information

This task is useful for determining the addresses associated with a node, without looking through configuration files. The information you see is real-time data taken from the node versus static information taken from a database.

Table 6.1-8 presents the procedures to view network address information in a condensed manner for quick reference. If you are already familiar with the procedures, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

Prerequisites for this Task

- The node must support SNMP.
- One or more SNMP nodes must be selected from the map. If you select more than one node, you receive a dialog box for each selected node.

- 1 Type **ovstart** at the command prompt and **press Enter**.
 - If the network management processes are not running, you can start them by executing the **\$OV_BIN/ovstart** command.
- 2 Type **ovstatus** at the command prompt and **press Enter**.
 - This command will check the status of the processes.
- 3 Type **x11start** at the command prompt and **press Enter**.
 - This command will start the X Windows session.
- 4 Type **ovw** at the command prompt and **press Enter**.
 - The **\$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
 - If the **\$OV_BIN** directory is not in your path, type **\$OV_BIN/ovw** to start HP OpenView Windows.
- 5 Select a **node** on the map.
- 6 Use the **Monitor: Network Configuration - Addresses....** Operation to view the following information about each interface on the node:
 - interface index
 - interface name
 - IP address
 - network mask
 - network address
 - link-level address (physical address)

For example:

Index	Interface	IP address	Network Mask	Network Address	Link Address
4	lan1	126.1.0.2	255.255.0.0	126.1.0.0	0x01002033333
3	lan0	126.1.0.3	255.255.0.0	126.1.0.0	0x01000202222
2	lo0	222.0.0.1	255.0.0.0	222.0.0.0	<none>

Table 6.1-8. Viewing Network Address Information- Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	ovstart \$OV_BIN/ovstart if network management processes are not running	press Enter
2	ovstatus	press Enter
3	x11start	press Enter
4	ovw \$OV_BIN/ovw if \$OV_BIN directory is not in the path	press Enter
5	Select a node on the map	select with mouse
6	Use the Monitor: Network Configuration - Addresses	select with mouse

6.1.5 Viewing How Traffic is Routed on a Network

This task lists the routing table information for a remote SNMP node. It can be useful in determining more efficient routes on the network, assessing the need for explicit routes and diagnosing connectivity problems. The information you see is real-time data taken from the node versus static information taken from a database.

Table 6.1-9 presents the procedures to view traffic routing in a condensed manner for quick reference. If you are already familiar with the procedures, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

When rerouting traffic on the network, there are two ways of performing the task:

- _ For temporary change, the command `route` command is used.
- _ For permanent change, `netlinkrc` needs to be edited and the system needs to be rebooted.

Prerequisites for this Task

- _ The node must support SNMP.
- _ One or more SNMP node must be selected from the map. If you select more than one node, you receive a dialog box for each selected node.

- 1 Type **ovstart** at the command prompt and **press Enter**.
 - _ If the network management processes are not running, you can start them by executing the **\$OV_BIN/ovstart** command.
- 2 Type **ovstatus** at the command prompt and **press Enter**.
 - _ This command will check the status of the processes.
- 3 Type **x11start** at the command prompt and **press Enter**.
 - _ This command will start the X Windows session.
- 4 Type **ovw** at the command prompt and **press Enter**.
 - _ The **\$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
 - _ If the **\$OV_BIN** directory is not in your path, type **\$OV_BIN/ovw** to start HP OpenView Windows.
- 5 Select a **node** on the map.
- 6 Use the **Monitor: Network Configuration - Routing Table..** operation to view the following information about each destination node with which the selected node communications:
 - _ destination name (default is a route that the system uses when it cannot find a specific route)

- _ name of the gateway (router) between the selected node and the destination
- _ type of route (for example, directly connected to a LAN, through a remote gateway, or route currently not available)
- _ network subnet mask associated with the route
- _ name of the interface that is used to reach the destination

Table 6.1-9. Viewing How Traffic is Routed on a Network- Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	ovstart \$OV_BIN/ovstart if network management processes are not running	press Enter
2	ovstatus	press Enter
3	x11start	press Enter
4	ovw \$OV_BIN/ovw if \$OV_BIN directory is not in the path	press Enter
5	Select a node on the map	select with mouse
6	Select Monitor: Network Configuration - Routing Table	select with mouse

6.1.6 Viewing the Services Available on a Node

This task lists the IP networking services for which a remote SNMP node is listening. It is useful for determining what configured services a node is currently running. The information you see is real-time data taken from the node versus static information taken from the database.

Table 6.1-10 presents the procedures to view available services on a node in a condensed manner for quick reference. If you are already familiar with the procedures, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

Prerequisites for this Task

- _ The node must support SNMP.
- _ One or more SNMP nodes must be selected from the map. If you select more than one node, you receive a dialog box for each selected node.

- 1 Type **ovstart** at the command prompt and **press Enter**.
 - _ If the network management processes are not running, you can start them by executing the **\$OV_BIN/ovstart** command.
- 2 Type **ovstatus** at the command prompt and **press Enter**.
 - _ This command will check the status of the processes.
- 3 Type **x11start** at the command prompt and **press Enter**.

- This command will start the X Windows session.
- 4** Type **ovw** at the command prompt and **press Enter**.
 - The **\$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
 - If the **\$OV_BIN** directory is not in your path, type **\$OV_BIN/ovw** to start HP OpenView Windows.
- 5** Select a **node** on the map.
- 6** Use the **Monitor: Network Configuration - Services..** operation, to view the following information about the selected node:
 - service protocol: either TCP (Transmission Control Protocol) or UDP (User Datagram Protocol).
 - Port to which the service is bound.
 - Service for which the node is listening (for example, telnet, nfs). If no service is listed, the service is either unavailable or unknown.

Table 6.1-10. Viewing the Services Available on a Node- Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	ovstart \$OV_BIN/ovstart if network management processes are not running	press Enter
2	ovstatus	press Enter
3	x11start	press Enter
4	ovw \$OV_BIN/ovw if \$OV_BIN directory is not in the path	press Enter
5	Select a node on the map	select with mouse
6	Select Monitor: Network Configuration - Services	select with mouse

6.2 Diagnosing Network Problems

A fault within network is defined as something that causes those systems “to fail to meet their operational objectives.” Three elements are involved in managing network faults: detection of the fault, isolation of the fault to a particular component, and correction of the fault. Fault management, therefore, may include the maintenance of error logs, error detection processes, and diagnostic testing procedures. For many managers, the term network management is synonymous with fault management.

Performance and fault management are difficult to separate. High performance usually implies a low incident of faults. Performance management, however, goes beyond minimizing faults; it is responsible for gathering statistics on the operation of the network, maintaining and analyzing logs of the state of the system, and optimizing network operation.

Sniffer Network Analyzer: Ethernet Monitor is used to make sure the network is working at its peak performance and will diagnose any possible fault within the network. The Ethernet Monitor is a network monitoring program. The monitor provides an accurate picture of network activity at any moment or a historical record on network activity over a period of time. This information helps you find traffic overloads, plan for network expansion, detect intruders, establish performance baselines, and distribute traffic more efficiently among servers and subnets.

The monitor's report capabilities let you communicate this information to others, complete with graphs and tables. The alarm capabilities alert you to problems with the network or with individual stations.

- _ This list summarizes the monitor's capabilities:
- _ Monitors up to 1,024 network stations
- _ Generates visible and audible alarms for the entire network or for individual stations
- _ Compiles a historical alarm log
- _ Provides real-time traffic and historical information for individual stations and for the entire network
- _ Sorts statistics to show only the items that interest you
- _ Creates customized management reports
- _ Automatically prints selected information at set time intervals

Note: The Ethernet Monitor only monitors frames on the Ethernet network segment to which the Network Interface Card is attached.

7. System Monitoring

7.1 Checking the Health and Status of the Network

Once a network has been discovered by **HP Open View IP discovery and layout**, monitoring the state of the network can begin. Monitoring includes tasks, such as, checking the map for color alerts which indicate problems, creating submaps needing special monitoring, and checking for network changes.

Objects that have an abnormal condition can be identified without having to look at every object on the network map. A color alert on a symbol indicates that some part of that object may have problems. To isolate a fault somewhere on the network, follow the color alerts to increasingly more specific submaps until the specific object that is not functioning is reached. Follow color alerts by opening child submaps of objects that contain a color alert.

The Activity Checklist table that follows provides an overview of the monitoring process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) number or Instruction (I) number where details for performing the task can be found. Column five (**Complete?**) is a checklist to keep track of which task steps have been completed.

Table 7.1-1. Monitoring - Activity Checklist

Order	Role	Task	Section	Complete?
1	Fault Manager	Starting NNM (Network Node Manger)	(P) 7.1.1	
1	Fault Manager	Verify that an object is not functioning	(P) 7.1.2	
2	Fault Manager	Looking at Maps for Color Alerts	(P) 7.1.3	
3	Fault Manager	Looking at Maps for New Nodes	(P) 7.1.4	
4	Fault Manager	Create Special Submaps for Monitoring Status	(P) 7.1.5	
5	Fault Manager	Checking for Event Notifications	(P) 7.1.6	
6	Fault Manager	Rediscovering Network	(P) 7.1.7	

Detailed procedures for tasks performed by the Fault Manger are provided in the sections that follow. The procedures assume the Network map is read-write, the IP map is enabled for the map, and is configured to display status. To interpret the meaning of status colors correctly, the compound status scheme of the open map should be known. This tells how status propagates from objects in a submap to the parent object. The compound status scheme for the map from the **Map Description** dialog box can be identified by selecting **File: Describe/Modify Map**.

Section 7.1.1 explains how to start NNM(Network Node Manager). Section 7.1.2 explains how to verify that an object is not functioning. Section 7.1.3 explains how to look at maps for color alerts. Section 7.1.4 explains how to look at maps for new nodes. Section 7.1.5 explains how to create special submaps for monitoring status. Section 7.1.6 explains how to check for event notifications. Section 7.1.7 explains how to rediscover the Network.

If you are already familiar with the procedures, you may prefer to use the quick-step tables. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented in Sections 7.1.1 through 7.1.5

7.1.1 Starting NNM (Network Node Manager)

HP Open View Network Node Manager is a set of applications that are integrated with HP Open View Windows (OVW). To Start NNM, HP Openview Windows must be activated first. Once activated, OVW will automatically start NNM. HP Openview windows will also automatically start the applications that are installed and registered.

Prerequisites for this Task

The network management processes that work with OVW and NNM must be running. The network management processes consist of the following HP OpenView background processes: **ovwdb, trapd, ovtopmd, ovactiond, snmpCollect, and netmon**. You can check to see if these processes are running with **/usr/ov/bin/ovstatus** command.

This procedure explains how to start the HP OpenView Windows graphical user interface.

- 1 Type **\$OV_BIN/ovstart** at the command prompt and **press enter**.
 - If the network management processes are not running, you can start them by executing the **\$OV_BIN/ovstart** command.
- 2 Type **ovstatus** at the command prompt and **press enter**.
 - This command will check the status of the processes.
- 3 Type **x11start** at the command prompt and **press enter**.
 - This command will start the X Windows session.
- 4 Type **\$OV_BIN/ovw** at the command prompt and **press enter**.
 - The **\$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
 - If the **\$OV_BIN** directory is not in your path, type **\$OV_BIN/ovw** to start HP OpenView Windows.
- 5 Type **ovw&** and **press enter**.
 - OVW displays the About OVW dialog box. After a few moments, you see the OVW Windows

To exit NNM and all other integrated applications, you must exit OVW. You can exit OVW in one of the following ways:

- 6 Select **File: Exit** from the menu bar of any submap window or go to step number 7;
- 7 **Click** on the **Close** button on all open submap windows until a black submap window is displayed. When the black submap window is displayed, click on the **Close** button.
 - The open map is saved, and all the submap windows and dialog boxes of the map are closed. OVW, all NNM applications, and all other integrated applications exit.

IMPORTANT: Do not use the quick step version of a procedure unless you are already very familiar with the procedure.

To start **NNM**, execute the steps provided in the table.

Table 7.1-1. Starting NNM - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	\$OV_BIN/ovstart	press Return
2	ovstatus	press Return
3	x11start	press Return
4	\$OV_BIN/ovw	press Return
5	ovw&	press Return

7.1.2 Verify That an Object Is Not Functioning

This section explains how to verify that an object is not functioning and assumes that HP Openview is running on the desktop. If not, then see section 7.1.1 To verify that an object is not functioning, any of the following procedures can be executed.

- 1 Select the **Monitor** pull down menu
- 2 Select **Device Configuration**
- 3 Select **System Information**

-or-

- 1 Select the **Diagnose** pull down menu
- 2 Select **Network Connectivity**
- 3 Select **Demand Poll**

-or-

- 1 Select the **Diagnose** pull down menu
- 2 Select **Network Connectivity**
- 3 Select **Ping**

If these operations do not produce any responses or they time out, then the node is probably down or otherwise unreachable over the network. See Section 7.1.5 Checking for Event Notifications to verify event status of the node. If a Fault has occurred see Section 8 on Problem Management and Section 21 COTS Hardware Maintenance.

IMPORTANT: Do not use the quick step version of a procedure unless you are already very familiar with the procedure.

To verify that an object is not working, execute the steps provided in the table.

Table 7.1-1. Verify - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	Monitor	Use the pull down menu
2	Device Configuration	Pull down menu
3	System Information	Pull down menu

7.1.3 Looking at Maps for Color Alerts

This example assumes that HP Openview is running on the desktop. If not, then see section 7.1.1 In this example, the Root submap is displayed, and a yellow Internet symbol is displayed on the Root submap. Compound status for the open map is set to HP Open View Window Default.

- 1 **Double click** on the yellow **Internet** symbol
 - The **Internet submap** opens and displays three IP networks attached to two gateways. One IP network symbol is yellow. This indicates a marginal problem with the network.
- 2 **Double click** on the yellow **IP network** symbol
 - A **Network submap** opens and displays three segments attached to two gateways. One segment symbol is yellow. This indicates a problem somewhere on the segment.
- 3 **Double click** on the yellow **segment** symbol
 - A **Segment submap** opens and displays the nodes attached to that segment. Of all the nodes in the segment, the workstation node is red. The problem is isolated to that workstation.
- 4 **Double click** on the red **workstation** symbol
 - A **Node submap** opens and displays two interface symbols, which indicate that two interfaces are installed on the workstation. One of them is red.
 - You have isolated the fault to a single card of a single node on your internet.

At this point see Section 8 on Problem Management and Section 21 COTS Hardware Maintenance.

IMPORTANT: Do not use the quick step version of a procedure unless you are already very familiar with the procedure.

To look at Maps for Color Alerts, execute the steps provided in the table.

Table 7.1-2. Color Alerts- Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	Internet Symbol	Double click
2	IP Network	Double click
3	Yellow segment symbol	Double click
4	Red workstation symbol	Double click

7.1.4 Looking at Maps for New Nodes

This section assumes that HP Openview is running on the desktop. If not, then see section 7.1.1 **IP Map** will automatically discover the **IP-addressable nodes** for the open map. The purpose of this section is to identify new objects that have been discovered and added to the open map. Because discovery is automated, additional symbols of objects on the network map will be seen. **IP Map** must be enabled for the map. This is the default. **IP Map** places new symbols directly on the submap if autolayout is enabled. IP Map places new symbols in the **New Object Holding Area** if autolayout is disabled for the submap.

- 1 To check the default **Segment submap** for any new nodes that may have been discovered, open the default **Segment submap** from the segment symbol in the Network submap.
 - View the submap for any new symbols.
- 2 To easily see new symbols in the submap, disable autolayout for the submap. When autolayout is disabled, a **New Object Holding Area** appears at the bottom of the submap.
 - All newly added symbols are placed in the **New Object Holding Area**.

7.1.5 Creating Special Submaps for Monitoring Status

This section assumes that HP Openview is running on the desktop. If not, then see section 7.1.1 Submaps can be created that are logically organized instead of physically organized. This will help to create logical submaps for specialized monitoring.

IMPORTANT: See section 4-5 of the **HP Openview Network Node Manager User's Guide** to use this feature.

7.1.6 Checking for Event Notifications

This section assumes that HP Openview is running on the desktop. If not, then see Section 7.1.1. Anytime a change occurs on the network an event is generated. Through the **Network Node Manager's** internal processes, the event is sent to a predefined category in the **Events Browser** window. The **Events Categories** window provides a notification of when new events occur. This window has a button corresponding to each of the event categories. When the button that corresponds to a specific event category is clicked, a window listing the events for that specific category appears. These windows are **Event Browser** windows. When a button in the **Event Categories** window changes color, it is an indication that an event occurred on the network which relates to that category. The color of the button indicates the highest severity event in the category. The default categories included in the **Event Categories** window are:

Error Events.	This indicates inconsistent or unexpected behavior.
Threshold Events.	This indicates that a threshold was exceeded.
Status Events.	This indicates an object or interface status changed to up or down, or an object or interface started or stopped responding to ICMP echo requests.
Configuration Events.	This indicates a node's configuration changed.
Application Alert Events.	This indicates an HP OpenView Window application generated an alarm or alert.
All Events.	This list all the above events and other events in one dialog box.

In the following example the **Threshold Events** button is red, which indicates that a critical threshold was exceeded somewhere on the network.

- 1 Click on the **Threshold Events** button in the **Event Categories** window. The **Threshold Events Browser** dialog box appears with a chronological listing of the threshold events that have occurred, with the most recent events at the bottom of the list.
 - Each event listed includes the severity, time the event occurred, node on which the event occurred, and a brief event message.
- 2 To view the node that generated the event shown in this example, select the event from the list and click on **Action → Highlight Source on Map**.
 - A map will appear with the **busynode** node highlighted. At this point, select the highlighted node by clicking on it, and invoke appropriate operations from the menu bar to further diagnose and correct the situation which caused the threshold to be exceeded.
- 3 To delete the event, select the event and click on **Action → Delete → Selected Event**.
 - This will delete only the selected event.

For more information about event notification, click on the **help** button in the dialog box for the event being viewed or select **View SNMP Events** from the **Help: Index → Task**

IMPORTANT: Do not use the quick step version of a procedure unless you are already very familiar with the procedure.

To check for **Event Notifications**, execute the steps provided in the table.

Table 7.1-6. Event Notifications - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	Threshold Events	press Return
2	Action	press Return
3	Highlight source on Map	press Return

7.1.7 Rediscovering the Network

This section assumes that HP Openview is running on the desktop. If not, then see section 7.1.1. Occasionally you may edit your maps beyond recognition and want to start from scratch.

- 1 Exit all Openview sessions (if running) **cd /usr/OV/bin** and then enter **ovstop** at the command line
 - This will stop all HP OpenView processes
- 2 Remove the Openview database (**do a backup first**)
 - **cd \$OV_DB/openview**
 - **rm -rf \$OV_DB/openview/***
- 3 Remove all of the current events.
 - **rm \$OV_LOG/xnmevents.***
 - **rm \$OV_LOG/trapd.log***
 - **rm \$OV_LOG/netmon.trace***
- 4 Clear the SNMP cache.
 - **cd /usr/OV/bin**
 - **xnmsnmpconf -clearCache**
- 5 Re register OVW fields.
 - **ovstart ovwdb**
 - **ovw -fields**
- 6 Restart NNM.
 - **ovstart**
 - **ovw &**

IMPORTANT: Do not use the quick step version of a procedure unless you are already very familiar with the procedure.

Table 7.1-7. Rediscovery - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	Stop all OVW sessions	select exit from pull down menu
2	ovstop	press enter
3	cd \$OV_BIN/openview	press enter
4	rm -rf \$OV_DB/openview/*	press enter
5	rm \$OV_LOG/xnmevents.*	press enter
6	rm \$OV_LOG/trapd.log*	press enter
7	rm \$OV_LOG/netmon.trace*	press enter
8	xnmsnmpconf -clearCache	press enter
9	ovstart ovwdb	press enter
10	ovw -fields	press enter
11	ovstart	press enter
12	ovw &	press enter

7.2 Tivoli Enterprise Console

The Tivoli Enterprise Console (TEC) provides centralized processing and management of distributed events, the ability to allow shared or partitioned administrator responsibilities based on enterprise-defined areas of responsibility, and a flexible interface to view and respond to events based on the events severity, source, location, or other characteristics. The following tables document the Tivoli event configuration.

Table 7.2-1. Disk Event Configuration (1 of 2)

Resource	Response Level	Trigger When	Threshold	Response
Inodes Free	Warning	Less than	200	Change icon.
	Severe	Less than	150	Send Tivoli notice. Change icon.
	Critical	Less than	100	Send Tivoli notice. Change icon. Popup alarm.
Inodes Used	Warning	Greater than	X	Change icon.
	Severe	Greater than	X	Send Tivoli notice. Change icon.
	Critical	Greater than	X	Send Tivoli notice. Change icon. Popup alarm.
% Inodes Used	Warning	Greater than	80	Change icon.
	Severe	Greater than	90	Send Tivoli notice. Change icon.

Table 7.2-1. Disk Event Configuration (2 of 2)

Resource	Response Level	Trigger When	Threshold	Response
	Critical	Greater than	95	Send Tivoli notice. Change icon. Popup alarm.
Space Free	Warning	Less than	200 MB	Change icon.
	Severe	Less than	100 MB	Send Tivoli notice. Change icon.
	Critical	Less than	50 MB	Send Tivoli notice. Change icon. Popup alarm.
Space Used	Warning	Greater than	X	Change icon.
	Severe	Greater than	X	Send Tivoli notice. Change icon.
	Critical	Greater than	X	Send Tivoli notice. Change icon. Popup alarm.
% Space Used	Warning	Greater than	80	Change icon.
	Severe	Greater than	90	Send Tivoli notice. Change icon.
	Critical	Greater than	95	Send Tivoli notice. Change icon. Popup alarm.
Tivoli DB Free Space	Warning	Less than	20 MB	Change icon.
	Severe	Less than	10 MB	Send Tivoli notice. Change icon.
	Critical	Less than	5 MB	Send Tivoli notice. Change icon. Popup alarm.

Table 7.2-2 Security Event Configuration (1 of 2)

Resource	Response Level	Trigger When	Threshold	Response
Check File Permission:				
/etc/passwd	Critical	Changes from	-rw-r--r--	Send Tivoli notice. Change icon. Popup alarm.
Compare Files:				
Daemon Status:				
amd	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
biod	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
cron	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
inetd	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
lockd	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
lpd	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
mountd	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
nfsd	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
portmap	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
snmpd	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.

Table 7.2-2 Security Event Configuration (2 of 2)

Resource	Response Level	Trigger When	Threshold	Response
statd	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
File Checksum:				
/etc/passwd	Warning	Not equal to	value	Change icon.
File Size:				
/var/adm/messages	Warning	Greater than	200 Kbytes	Change icon.
Occurrences in File:				
/var/adm/messages	Warning	Greater than	value	Change icon.
Process Instances:				
tivoli	Warning	Greater than	3	Change icon.
HP OpenView	Warning	Greater than	3	Change icon.
User Logins by User:				
root	Warning	Greater than	1	Change icon.
Users Logged in	Warning	Greater than	20	Change icon.
	Severe	Greater than	25	Send Tivoli notice. Change icon.
	Critical	Greater than	30	Send Tivoli notice. Change icon. Popup alarm.

Table 7.2-3. Network Event Configuration (1 of 3)

Resource	Response Level	Trigger When	Threshold	Response
Client RPC timeouts	Warning	% increase of	10	Change icon.
	Severe	% increase of	25	Send Tivoli notice. Change icon.
	Critical	% increase of	50	Send Tivoli notice. Change icon. Popup alarm.
Server Status				
Network Collisions	Warning	% increase of	5	Change icon.
	Severe	% increase of	10	Send Tivoli notice. Change icon.
	Critical	% increase of	25	Send Tivoli notice. Change icon. Popup alarm.

Table 7.2-3. Network Event Configuration (2 of 3)

Resource	Response Level	Trigger When	Threshold	Response
Network Collisions/packets	Warning	% increase of	5	Change icon.
	Severe	% increase of	10	Send Tivoli notice. Change icon.
	Critical	% increase of	25	Send Tivoli notice. Change icon. Popup alarm.
NFS bad calls	Warning	% increase of	10	Change icon.
	Severe	% increase of	25	Send Tivoli notice. Change icon.
	Critical	% increase of	50	Send Tivoli notice. Change icon. Popup alarm.
Input packet errors	Warning	% increase of	10	Change icon.
	Severe	% increase of	25	Send Tivoli notice. Change icon.
	Critical	% increase of	50	Send Tivoli notice. Change icon. Popup alarm.
Input packets	Warning	% increase of	10	Change icon.
	Severe	% increase of	25	Send Tivoli notice. Change icon.
	Critical	% increase of	50	Send Tivoli notice. Change icon. Popup alarm.
Output packet errors	Warning	% increase of	10	Change icon.
	Severe	% increase of	25	Send Tivoli notice. Change icon.
	Critical	% increase of	50	Send Tivoli notice. Change icon. Popup alarm.
Output packets	Warning	% increase of	10	Change icon.
	Severe	% increase of	25	Send Tivoli notice. Change icon.
	Critical	% increase of	50	Send Tivoli notice. Change icon. Popup alarm.

Table 7.2-3. Network Event Configuration (3 of 3)

Resource	Response Level	Trigger When	Threshold	Response
Remote oserv status	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
RPC bad calls	Warning	% increase of	10	Change icon.
	Severe	% increase of	25	Send Tivoli notice. Change icon.
	Critical	% increase of	50	Send Tivoli notice. Change icon. Popup alarm.

Table 7.2-4. System Event Configuration (1 of 2)

Resource	Response Level	Trigger When	Threshold	Response
Available swap space	Warning	Less than	20 MB	Change icon.
	Severe	Less than	15 MB	Send Tivoli notice. Change icon.
	Critical	Less than	10 MB	Send Tivoli notice. Change icon. Popup alarm.
Host status:				
cyclops	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
Lingering terminated processes	Warning	Greater than	10	Change icon.
	Severe	Greater than	20	Send Tivoli notice. Change icon.
	Critical	Greater than	30	Send Tivoli notice. Change icon. Popup alarm.
Load average	Warning	Greater than	10	Change icon.
	Severe	Greater than	20	Send Tivoli notice. Change icon.

Table 7.2-4. System Event Configuration (2 of 2)

Resource	Response Level	Trigger When	Threshold	Response
	Critical	Greater than	30	Send Tivoli notice. Change icon. Popup alarm.
Mail queue length	Warning	Greater than	20	Change icon.
	Severe	Greater than	40	Send Tivoli notice. Change icon.
	Critical	Greater than	50	Send Tivoli notice. Change icon. Popup alarm.
Page-outs	Warning	% increase of	50	Change icon.
	Severe	% increase of	80	Send Tivoli notice. Change icon.
	Critical	% increase of	90	Send Tivoli notice. Change icon. Popup alarm.

Table 7.2-5 Printer Event Configuration (1 of 2)

Resource	Response Level	Trigger When	Threshold	Response
Daemon status:				
lpsched	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
Jobs in print queue:				
print_queue	Warning	Greater than	10	Change icon.
Status of print queue:				
print_queue	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.

Table 7.2-5 Printer Event Configuration (2 of 2)

Resource	Response Level	Trigger When	Threshold	Response
Total size queued:				
print_queue	Warning	Greater than	10 M	Change icon.
	Severe	Greater than	20 M	Send Tivoli notice. Change icon.
	Critical	Greater than	30 M	Send Tivoli notice. Change icon. Popup alarm.

X - system dependent parameters.

This page intentionally left blank.

8. Problem Management

The Trouble Ticket System is the vehicle to record and report M&O problems during the operational phase. Trouble tickets can be generated by operations, maintenance, and customer personnel as well as users. The Trouble Ticket System is automated and all problem resolution activities are recorded in the database tool, the Remedy Action Request System. Documentation that is not in electronic form is handled by the local Performance Assurance Analyst and is listed as an attachment to the trouble ticket.

A CM Administrator (site or system-level) is assigned to serve as a Trouble Ticket database administrator. The CMA is responsible for tracking ECS system-level issues discovered at the sites and for propagating system problem resolutions to the site level. The CMA also supports the activities of the Trouble Ticket Review Board. This includes generating status reports, and distributing resolutions, instructions, and changes as directed by the Board. User Services Representatives monitor trouble tickets to notify users concerning problem resolution and status. Problem investigator records and updates all activities in the trouble ticket. This information can be used to determine critical maintenance concerns related to frequency of occurrence, criticality level, and the volume of problems experienced. The maintainability analysis will guide critical changes, volume and type of support components to be utilized, and will focus further ECS release development.

8.1 Problem Resolution Process — An Overview

DAAC personnel will submit trouble tickets via Remedy. Trouble tickets are first evaluated by the Ops Controller to determine the severity and cause of the problem as the basis for assignment of priority and on-site resolution responsibility/cognizance. Every trouble ticket is logged into the database for record keeping purposes. Trouble tickets that can be resolved locally are assigned and tracked at the local center. Matters of sufficient importance are escalated to the System Trouble Ticket Telecon agenda for further discussion and disposition.

System level review board includes the SEO TT process. Trouble Tickets are discussed at a weekly trouble ticket Telecon. This meeting functions as the ECS Failure Review Board in compliance with the *EOS Performance Assurance Requirements for ECS*, GSFC 420-05-03, Section 7.12.2.2. The telecon is held to coordinate trouble ticket activities within the system and site M&O organization as well as with development, customer, and user organizations. Attendees include: Customer representatives; ECS SEO engineering teams leads (one is designated as chairperson of the meeting); ECS ILS engineering support; ECS DAAC engineering team leads and operations representatives; ECS M&O support staff; ECS development organization representatives (including management, technical, configuration management and quality assurance); SCF(s) representatives.

Agenda items may be supplemented or replaced by hardcopy or softcopy reports. Material from this meeting is distributed within each ECS organization and to customer and user organizations as required. A typical agenda might include:

- Review and prioritize (system-level) each trouble ticket opened at each center.
- Review and re-prioritize older trouble tickets (as required).
- Assign trouble ticket work-off responsibility to one organization.
- Review distribution of trouble tickets by organization, priority and age.
- Discuss trouble ticket issues with development organizations.

The Maintenance & Operations Problem Management Concept is outlined in the following procedures, which are illustrated in Figures 8.1-1 and 8.1-2:

1. User or Operator discovers a problem with ECS configuration item(s) (hardware, software, documentation, procedure) and documents this problem for later resolution. A user submits to User Services: by calling up the Trouble Ticket System via the Internet (see Section 8.3, below); by going on-line with the Trouble Ticket database (Remedy) ; by phoning User Services; or by sending an e-mail message to Remedy. (See Section 8.2.2.) Operators document problems directly via Remedy.
2. The trouble ticket is logged into the system. Remedy automatically assigns "New" status to the trouble ticket and notifies the Operations Controller for assignment and prioritization. Remedy notifies the Operations Controller via email, or through Remedy's notification tool, or both (see Section 8.2.1.4). Trouble tickets are subsequently statused and reported by the CMA.
3. The trouble ticket is prioritized according to a system of operational priorities. The Performance Assurance Requirements document, NASA 420-05-03, identifies problem priorities; which correspond to the triage system of maintenance priorities:

Priority / Category 1: System/Service cannot perform critical function or imposes major safety hazard.

Presents accomplishment of critical operations tasks (tasks identified in separately maintained lists); imposes major safety hazard to personnel, systems, or space mission resources; or results in loss of one or more essential mission objectives.

Priority / Category 2: System/Service substantially impaired.

Substantially impacts critical functions/prevents accomplishments of non-critical functions; fails to operate within critical performance specifications; or cannot effectively or efficiently fulfill baseline requirements.

Priority / Category 3: System/Service slightly impaired.

Causes minor or no substantial impact to development, operations, services, or data processing functions. Support may be degraded, but mission can still be accomplished.

The Trouble Ticket System tool (Remedy) has coded the triage as HIGH, MEDIUM, and LOW. The User can designate a priority level for the problem. However, the official priority is assigned by the Operations Controller and maintained by the CM Administrator. All Category 1 (Priority 1) trouble tickets will be elevated to the Government Failure Review Board and will require both Government and Contractor Project Manager approval for final close-out. The sites and SEO apply these additional priorities:

Priority 4: Nuisance Problem: Includes the arrangement of video screens, color, and so on.

Priority 5: Closed Problem: A known issue with a prior disposition.

4. All potentially affected Operations Controller at other sites (SMC, DAACs, EOC, EDF) are notified of the problems with potential system impact and may provide inputs to problem assessment (impact) and resolution.
5. The Trouble Ticket database is updated with inputs received by the Operations Supervisor, and the trouble ticket may be modified to reflect this new information/coordination activity.
6. The Operations Controller assigns the problem to a Problem Investigator for analysis/resolution.
7. The Problem Investigator is responsible for problem investigation, proposed resolution and coordinates input from SEO, developers, vendors, and external organizations to effect the local resolution. The Problem Investigator presents significant issues at the contractor Telecon sponsored by SEO.
8. The Problem Investigator updates the trouble ticket database.
9. The Problem Investigator forwards any information regarding proposed/implemented fixes to the established notification list.
10. The proposed resolution is then presented to the DAAC Trouble Ticket Review Board (and Government Failure Review Board for Priority 1) for review, ratification, or revision.
11. Changes that do not affect configuration controlled items may be approved and implemented by the Failure Review Board/Trouble Ticket Review Board and closed only by operations lead approval. CCR's must be written and CCBs must approve changes that affect configuration controlled items. Temporary changes are updated in Baseline Manager (see Section 9.9 of this document). Permanent changes are proposed in a CCR to either on-site or system-level CCBs. Emergency fixes can be made and then reported to the CCB after the crisis is resolved. (See Section 8.4.)
12. The CCBs may approve, reject, or revise the change proposal.

13. On-site staff will be assigned to implement approved TT and some approved CCR solutions. After the solution is implemented and documented in the TT (the TT is submitted to the TTRB for closure.
14. The off-site problem resolution process will be managed by the SEO Trouble Ticket Review Board, who may also revise the on-site proposed solution because of any system-level effect(s). This is part of the problem escalation process which also includes appropriate submission of CCR(s).
15. The CCR may be escalated to higher level CCBs for system and/or external elements involved in the resolution process.

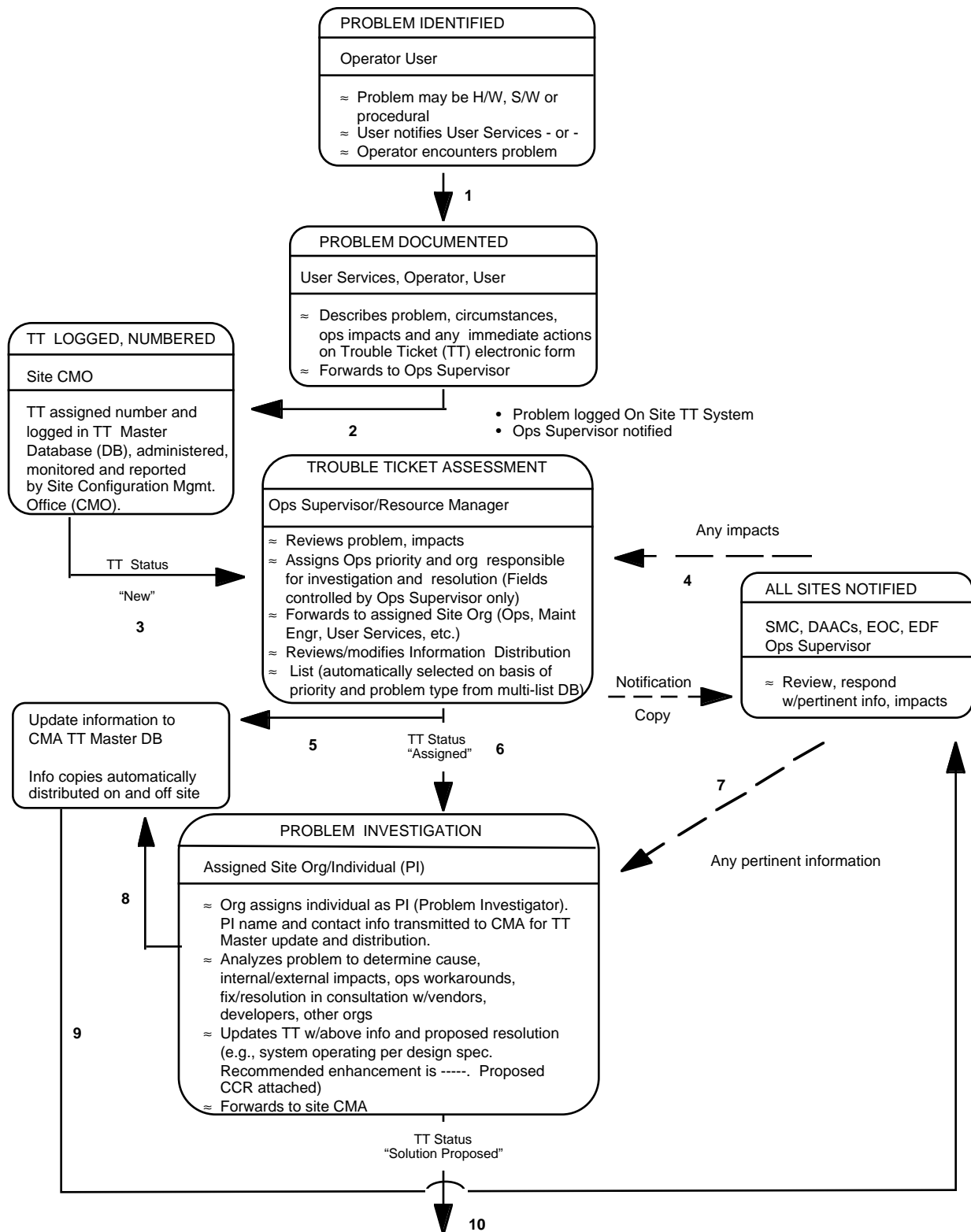


Figure 8.1-1. ECS Problem Management Concept - Part I

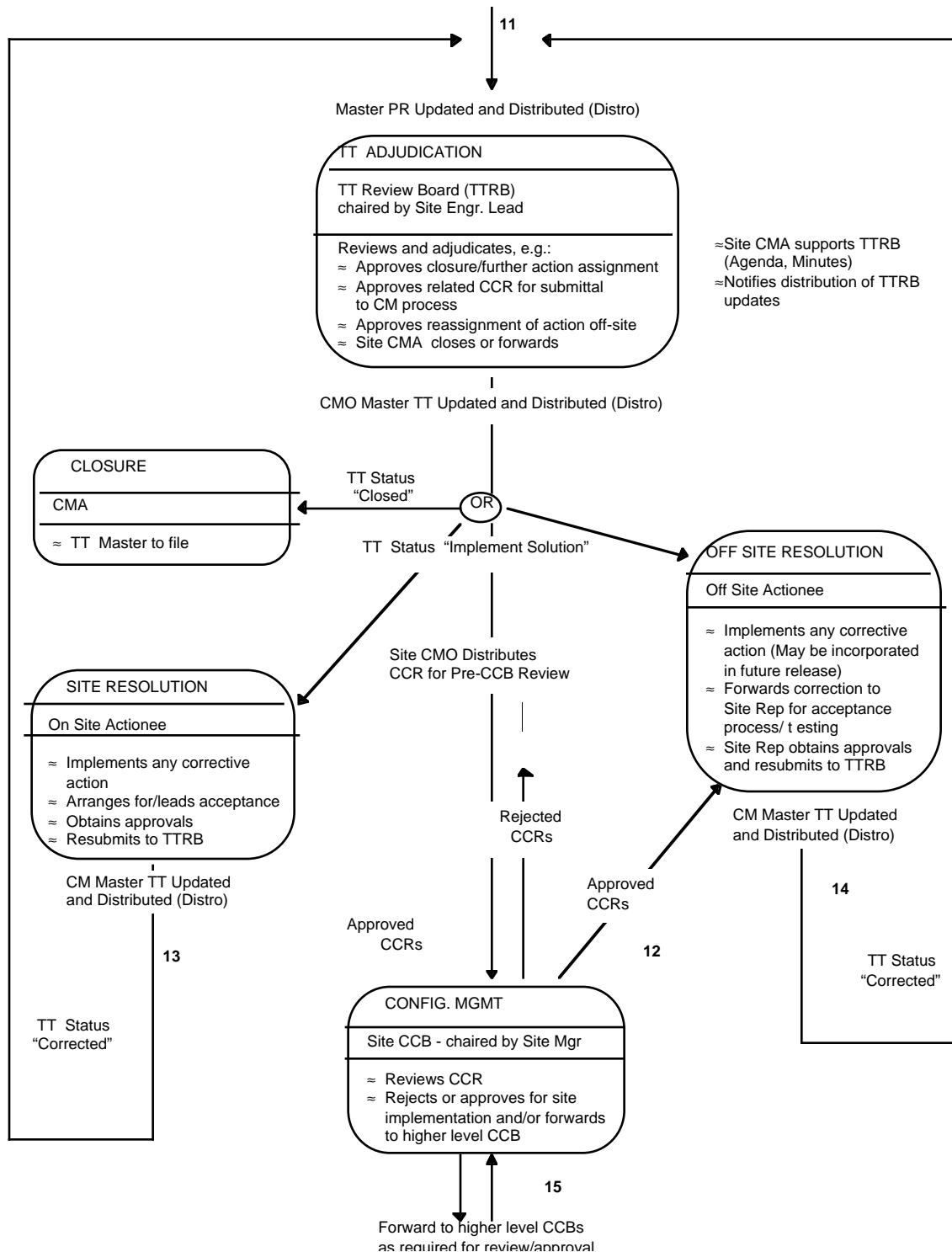


Figure 8.1-2. ECS Problem Management Concept - Part II

8.2 Using the Trouble Ticket System Tool

The Remedy Action Request System provides a distributed Trouble Ticketing Service that furnishes DAACs a common environment and means of classifying, tracking, and reporting problem occurrence and resolution to both ECS users and operations personnel. The Trouble Ticketing Service:

- _ Provides a GUI for operations personnel to access all Trouble Ticket services.
- _ Provides a common Trouble Ticket entry format.
- _ Stores Trouble Tickets.
- _ Retrieves Trouble Tickets via ad hoc queries.
- _ Allows operations personnel to forward problems from one site to another.
- _ Produces stock and common reports.
- _ Interfaces with user's and operator's e-mail to provide automatic notification.
- _ Offers an application programming interface through which applications can submit trouble tickets.
- _ Provides summary information to the SEO from each DAAC to allow trend reports regarding trouble tickets.
- _ Defines a consistent "life cycle" for trouble tickets.
- _ Allows each DAAC a degree of customization through definition of further re-prioritization and action rules.

Rules for re-prioritization are time-activated events, which execute on trouble tickets that meet a set of specified criteria (see Section 8.2.9, below). Actions which can be taken include notification (either to a user or to a support staff member), writing to a log file, setting a field value on the trouble ticket, or even running a custom written process. Qualifications can be expressed on any trouble ticket data tracks. Active links are similar to escalation rules with the exception that they are defined to take place on a specified action rather than at a given time.

Sections 8.2.1 through 8.2.9 provide procedures using Remedy. If you need more information about using HTML, see Section 8.3, below. For more information using Remedy, see the Remedy User's Guide.

The Activity Checklist table that follows provides an overview of the Trouble Ticket System. Column one (**Order**) shows the order in which tasks might be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three

(**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 8.2-1. Trouble Ticket System - Activity Checklist

Order	Role	Task	Section	Complete?
1	ECS users	Access the Trouble Ticket System	8.2.1, 8.3.1	
2	ECS users	Submit Trouble Ticket	8.2.2	
3	Problem Investigator	Modify Open Trouble Ticket	8.2.3	
4	Operations Controller, Problem Investigator	Forward Trouble Ticket	8.2.4	
5	Performance Analyst	Add Users to Remedy Upon Approval From Ops. Lead	8.2.5	
6	Performance Analyst	Modify Remedy User Privileges, Upon Approval From Ops. Lead	8.2.6	
7	Performance Analyst	Modify Remedy's Configuration, Upon Approval From Ops. Lead	8.2.7	
8	CMA	Generate Reports	8.2.8	
9	CMA	Maintain Escalation Time Table	8.2.9	
10	Ops. Supervisor Eng. Lead	Close Trouble Tickets	8.1	

8.2.1 Accessing the Trouble Ticket System

The Trouble Ticket System is accessed through either HTML or Remedy. The Trouble Ticket HTML is used by both User Services and the end user to submit trouble tickets without going through Remedy. It is accessed by clicking on the Trouble Ticket icon. Through HTML, the user can submit, obtain a list, and view details of trouble tickets.

Through Remedy, the User clicks on the User Tool icon, which opens the RelA-Trouble Tickets schema to submit, query, or work a Trouble Ticket. The Main Remedy Trouble Ticket screen is used to select the appropriate schema for submitting, modifying, or displaying a trouble ticket. The Main Page data fields are identified in Table 8.2-2.

The Pre-RelB-Trouble Tickets Schema provides the following options, which are initiated by clicking on the appropriate button:

— **Forward** -- Forwards this Trouble Ticket to the site specified in the "Forward-to" field.

— **Hardware Information** -- Opens a window that is associated with this Trouble Ticket to hold hardware information. (See Section 8.2.1.3.)

– **List All Masters** -- All Trouble Tickets that are duplicates of each other have one master. This button will lists all master Trouble Tickets.

– **List This Trouble Ticket's Duplicate(s)** -- List all Trouble Tickets that have duplicates associated to this Trouble Ticket.

– **Go to Contact Log** -- If this Trouble Ticket was created from a Contact Log, then this button will open a window to that Contact Log.

Several time-saving features are available through Remedy: the Admin Tool, GUI Import tool, the Hardware Information schema, and the GUI Notification tool. Brief descriptions are provided in Sections 8.2.1.1 through 8.2.1.4.

Table 8.2-2. Pre-RelB-Trouble Ticket Field Description (1 of 2)

Field Name	Data Type	Size	Entry	Description
Ticket-Id	Character	15	System generated	Ticket number which is set and maintained by the system
Ticket Status	Selection	4	Required	Status of the Trouble Ticket
Assigned-Priority	Selection	4	Required	Priority of Trouble Ticket assigned at the site (HIGH, MEDIUM, LOW)
Short Description	Character	128	Required	Short Description of the problem
Submitter Impact	Selection	4	Optional	Impact of the problem to the submitter
Long-Description	Character	255	Optional	Long Description of the problem
Resolution Log (End User Sees)	Diary	Unlim	Optional	General steps in the resolution of the problem
Detailed Resolution Log	Diary	Unlim	Optional	Detailed steps in the resolution of the problem
Submitter ID	Character	30	Required	User Id of the Submitter.
Submitter Name	Character	30	Optional	Full Name of the Submitter
Submitter Phone	Character	30	Optional	Phone number of the Submitter
Submitter eMail	Character	64	Optional	E-mail address of the Submitter
Submitter Home DAAC	Character	60	Optional	Home DAAC of the Submitter
History	Diary	Unlim	Optional	Upon submission or modification, the person assigned to the ticket and the ticket status will be indicated in the History field. Due to a limitation in Remedy, this information will only be written when the Assigned-to and Status fields are modified
Assigned-To	Character	30	Optional	Person that Trouble Ticket has been assigned to
Last-modified-by	Character	30	System generated	Person that last modified the Trouble Ticket
Create-date	Date/Time	4	System generated	Date Trouble Ticket was created at the present site

Table 8.2-2. Pre-RelB-Trouble Ticket Field Description (2 of 2)

Field Name	Data Type	Size	Entry	Description
Last-Modified-date	Date/Time	4	System generated	Date the Trouble Ticket was last modified
Related CCR	Character	60	Optional	ID of a related CCR
Key Words	Character	255	Optional	Key words to help identify this Trouble Ticket
Problem Type	Character	30	Optional	Type of problem addressed by this Trouble Ticket
Closing Code	Character	60	Optional	Origin of the problem that this Trouble Ticket resulted from
Closed-by	Character	60	Optional	Person that closed this Trouble Ticket
Close-date	Date/Time	4	Optional	Date this Trouble Ticket was closed
Software Resource	Character	60	Optional	Software Resource that the problem came from
Hardware Resource	Character	60	Optional	Hardware Resource that this problem came from
Duplicate Master Id	Character	25	Optional	The Master Ticket-ID of this Trouble Ticket
Forward-to	Character	60	Optional	Site that this Trouble Ticket was last forwarded to
Forwarded-from	Character	60	Optional	Site that forwarded this Trouble Ticket
Forwarded-by	Character	60	Optional	Contact person at the forwarding site
Forward-date	Date/Time	4	Optional	Date Trouble Ticket was forwarded
Unique-Identifier	Character	20	Optional	Unique identifier which is established at the origination site This identifier should NEVER be changed once set
Forwarded-to-1	Character	60	Optional	First site to have been forwarded this Trouble Ticket
Forwarded-to-2	Character	60	Optional	Second site to have been forwarded this Trouble Ticket
Forwarded-to-3	Character	60	Optional	Third site to have been forwarded this Trouble Ticket
Forwarded-to-4	Character	60	Optional	Fourth site to have been forwarded this Trouble Ticket
Associated Contact Log Id	Character	30	Optional	ID number of the Associated Contact Log

8.2.1.1 Remedy's GUI Admin Tool

The Admin Tool is used to notify or set fields as soon as the trouble ticket reaches a particular state or to escalate the problem once a trouble ticket is in a particular state too long. This tool is accessed in two ways:

1. By clicking on Admin Tool to open correct filter, escalation, or active link. (Problem escalation is discussed in Section 8.2.9.)
2. By clicking on User Tool icon and opening Pre-RelB-TT-Times schema to review/modify a Trouble Ticket.

For more information on the Admin Tool, refer to the Remedy Administration Manual.

8.2.1.2 Remedy's GUI Import Tool

The GUI Import tool is used to import existing entries rather than retyping information manually. It also enables the user to import entries into a schema from a file generated by the Admin tool. This tool is accessed by clicking on the Remedy Import Tool icon. For more information on the Import tool, refer to the Remedy User Guide.

8.2.1.3 Remedy's Hardware Information Schema

If detailed hardware information needs to be provided beyond what can be entered on the Trouble Tickets schema. The User Tool, Hardware Information schema, provides the vehicle to add a description of a hardware problem that corresponds to a trouble ticket. Through this schema, the user can enter detailed information about failed hardware components (e.g., part and serial numbers) and the actions taken to correct the problem. This schema is accessed by clicking on the User Tool icon and opening RelA-Hardware Information schema, or via Hardware Information link from Trouble Tickets schema.

8.2.1.4 Remedy's GUI Notification Tool

The GUI Notification Tool is used as an alternative to email notification to notify the user of a Remedy event. This tool is accessed by clicking on the Remedy Notification Tool icon. It allows properties and options to be modified via pull-down menus. Examples of GUI notification include a beep, a pop-up window, a flashing message. In addition, both an email and a GUI notification can be sent if the site so desires.

8.2.2 Submit a Trouble Ticket

When a problem is either found by or reported to User Services, follow the procedure applicable to your system, to create and log trouble tickets. Trouble tickets can be submitted via HTML or via Remedy's user tool – Pre-RelB Trouble Tickets schema. Remedy's Contact Log schema is used to classify, track, and report contacts of ECS users and operators and also to submit a trouble ticket from a log entry. E-mail is another method of submitting a trouble ticket. The template is available from your System Administrator.

1. For HTML submission:
 - a) Access HTML Trouble Ticketing Main page. Click on Trouble Ticket icon from the ECS desktop.
 - b) Select Submit link which opens the Submit page.

- c) Fill out the impact, short description, and detailed description fields.
 - d) Select Submit.
- 2. For submission through Remedy (See the Remedy User Guide, Chapter 3, “Submitting an Action Request” for the general steps):
 - a) Access Remedy User Tool (See the Remedy User Guide, Chapter 2, “Getting Started with the User Tool”, page 2-3, section on “Starting the User Tool”).
 - b) Access RelA-Trouble Ticket schema (See the Remedy User Guide, Chapter 2, “Getting Started with the User Tool”, page 2-18, section on “Using Schemas”).
 - c) Select Open Submit from the File menu.
 - d) Fill out at least Short Description and User Identification.
 - e) Fill out any other pertinent fields.
 - f) Select Apply.
- 3. For submission from a Remedy Contact Log entry:
 - a) Click on User Tool icon and open Pre-RelB-Contact Log schema.
 - b) Fill out Contact Log ID and Contact Information. If the contact is a registered Remedy user, the contact information is filled out automatically.
 - c) Fill in Short Description (limit is 128 characters).
 - d) Click on **Create TT** button.
- 4. For submission via E-mail: **This feature does not exist in the Pre-Release B Testbed.**
 - a) Obtain Template from your System Administrator.
 - b) Address the message to arsystem@_____._____.
 - c) Copy template into message area. **DO NOT INCLUDE AS AN ATTACHMENT. DO NOT ALTER TEMPLATE.** The template is presented in Figure 8.2.2-1. The # sign indicates comments, which are not read by Remedy. **Enter data as indicated in Figure 8.2.2-1.** Send message.

```

#
#  File exported Wed Feb 28 19:01:27 1996
#
Schema: RelA-Trouble Tickets
Server: remedy server name
Login:
Password:

```

	Field	ID
Short Description !	8!:	
Submitter Impact !536870922!:	Low	
# Values: Low, Medium, High		Select
Long-Description !	9!:	
Submitter ID !	2!:	
Submitter Name !536870917!:		Enter data
Submitter Phone !536870918!:		
Submitter eMail !536870921!:		
Submitter Home DAAC !536870919!:		

Figure 8.2-1. Trouble Ticket E-mail Template

8.2.3 Reviewing and Modifying Open Trouble Tickets

Trouble tickets may need to be modified based on better understanding of the nature of problems defined and revised resolutions from the Maintenance Engineer investigations, Sustaining Engineering inputs, Developer inputs, Trouble Ticket Review Board decisions, Change Control Board decisions, and/or Failure Review Board decisions. The results will be factored into revisions and/ or additions to the Trouble Ticket log.

1. For Review and Modification of Trouble Tickets:
 - a) Access Trouble Ticketing Main (see Section 8.3). Trouble Tickets can be *submitted, queried or modified*.
 - b) Select List link which opens the List page and shows each Trouble Ticket's Identification, Short Description, and Status.
 - c) Select the Trouble Ticket Id to get a more detailed description of that particular Trouble Ticket.
2. For Reviewing and Modifying Trouble Tickets through Remedy (See the Remedy User Guide, Chapter 4, "Reviewing and Modifying Action Request" for the general steps):
 - a) Access Remedy User Tool (See the Remedy User Guide, Chapter 2, "Getting Started with the User Tool", page 2-3, section on "Starting the User Tool").
 - b) Access Release A-Trouble Ticket schema (See the Remedy User Guide, Chapter 2, "Getting Started with the User Tool", page 2-18, section on "Using Schemas").
 - c) Select List from the Query menu.
 - d) From the List pick the Trouble Ticket(s) that you would like to Review/Modify.
 - e) Select Modify Individual from the Query menu of the List window review and modify Trouble Ticket.

8.2.4 Forwarding Trouble Tickets

Trouble ticket administrative reports are forwarded for local and system-wide usage. The trouble ticket contains all forwarding information; once forwarded, it goes to the Pre-RelB-TT-Forward-To-Site holding area (transparent to the user). The Pre-RelB-TT-Sites schema is used to indicate the site name and email address to be used in forwarding. To forward a trouble ticket:

1. Click on User Tool icon and open Pre-RelB-Trouble Ticket schema.
2. Set the status to "Forwarded".
3. Select a value for the Forward-to field from its picklist.
4. Select the Forward button.
5. Select Apply.

If necessary, a site name and email address can be modified, added, or deleted to update the picklist of Release A sites by authorized Remedy users: DAACs, SMC, NSI, EBnet. To modify picklist:

1. Click on User Tool icon and open Pre-RelB-TT-Sites schema.
2. Modify data.

8.2.5 Adding Users to Remedy

The Performance Assurance Analyst uses the Pre-RelB-User schema to grant access to the Remedy tool. See Remedy Administrator's Guide for OSF/ Motif, Chapter 3, "Setting Up Users and Groups", page 3-11, section on "Adding Users". Users who change jobs can be deleted.

8.2.6 Changing Privileges in Remedy

This procedure is used by the CM Administrator to control privileges of those who have been granted access. For more information, refer to the Remedy Administrator's Guide.

NOTE: No group should be modified without proper configuration change approval.

To change Privileges in Remedy:

1. See Remedy Administrator's Guide, Chapter 3, "Setting Up Users and Groups", page 3-2, section on "Understanding Access Control".
2. See Remedy Administrator's Guide, Chapter 3, "Setting Up Users and Groups", page 3-4, section on "Access Control Groups".
3. Groups have already been created to accommodate all privileges needed by Remedy Users for Release A. These groups are identified in see Table 8.2-3.

Table 8.2-3. Table of Access Control Groupings (1 of 2)

Groups	Description	Access Type
Operator	Submits trouble ticket internally.	Change
User Services	Submits trouble ticket internally for user.	Change
Operations Controller	Assigns problem priority and resolution responsibility. Can forward trouble ticket to another site.	Change
Resolution Technician	Attempts to resolve problem.	Change
Trouble Ticket Review Board Chair Person	Reviews proposed solutions. Approves reassignments, closures	Change
Administrator	Adds groups and users. Changes permissions. Sets escalation times. Sets menu items. Etc.	Change
Browser	Read only permission.	Read
Customize	Can use all features of the customize facility.	Change
Submitter	Place holder for anyone that submits a trouble ticket.	NA
Assignee	Place holder for anyone that is assigned a trouble ticket.	NA
Public	Read only permission. Guest users are automatically put in this group.	Read
NotifyNewEscal	Everyone that will be notified on an escalation due to trouble ticket being in "New" status.	Read

Table 8.2-3. Table of Access Control Groupings (2 of 2)

Groups	Description	Access Type
NotifyAssignedEscal	Everyone that will be notified on an escalation due to trouble ticket being in "Assigned" status.	Read
NotifySolPropEscal	Everyone that will be notified on an escalation due to TT being in "Solution Proposed" status.	Read
NotifyImpSolEscal	Everyone that will be notified on an escalation due to trouble ticket being in "Implement Solution" status.	Read
NotifySolImpEscal	Everyone that will be notified on an escalation due to TT being in "Solution Implemented" status.	Read

8.2.7 Modifying Remedy's Configuration

Pre-RelB-Trouble Ticket schemas' pulldown menus can be customized. Customization is achieved through the User Tool by modifying the Pre-RelB-Menu-Closing Codes, Pre-RelB-Menu-Hardware Resources, Pre-RelB-Menu-Software Resources, Pre-RelB-Menu-Key Words, Pre-RelB-Menu-Problem Type, Sites schemas.

To modify the Remedy environmental variables, refer to the Remedy User's Guide and Remedy Administrator's Guide as indicated.

1. See Remedy User's Guide, Chapter 7, "Customizing the Environment."
2. See Remedy Administrator's Guide, Chapter 1, "Using the Administrator Tool."

NOTE: No administrative configuration should be made without proper configuration change approval.

8.2.8 Generating Trouble Ticket Reports

A set of predefined reports will be placed in a public directory that should be downloaded to your personal configuration directory (see the Remedy User Guide, Chapter 2, "Getting Started with the User Tool," page 2-31, section "Sharing Macros, User Commands and Custom Reports," sub-section "Copying Files"). These reports are trouble ticket administrative reports generated for local and system-wide usage. See Remedy User's Guide, Chapter 5, "Reports."

8.2.9 Re-prioritization of Dated Trouble Ticket Logs

Remedy provides automated prioritization of trouble tickets based on delinquency status of out-dated trouble ticket logs. The File Tickler System automatically assigns higher priority to promote timely resolution.

1. Access Remedy User Tool (See the Remedy User Guide, Chapter 2, "Getting Started with the User Tool," page 2-3, section on "Starting the User Tool").

2. Access Pre-RelB-Times schema (See the Remedy User Guide, Chapter 2, “Getting Started with the User Tool”, page 2-18, section on “Using Schemas”).
3. Select List from the Query menu.
4. From the List pick the Time(s) that you would like to Review/Modify.
5. Select Modify Individual from the Query menu of the List window to review and/or modify the Time (in seconds).

8.3 Using Hypertext Mark-up Language (HTML) Screens

THIS SECTION IS NOT A PART OF THE PRE-RELEASE B TESTBED BUT WILL BE INCLUDED IN RELEASE B.

The hypertext mark-up language (HTML) Trouble Ticket Main Screen (“ECS Trouble Ticketing: Menu”) provides an introduction on how to use the Trouble Ticketing HTML, and is used by registered ECS users to go to either the Submit page or List page.

Selecting **Submit a Trouble Ticket** will bring up the Trouble Ticketing Submit screen.

Selecting **List the [username] Trouble Tickets** will bring up the Trouble Ticketing List screen.

Help on the Trouble Ticket HTML screens is available by clicking on the Trouble Ticket Help icon at the bottom of the screen .

8.3.1 ECS Trouble Ticketing HTML Submit Screen

The HTML Trouble Ticket Submit screen is used by registered ECS users to submit a Trouble Ticket.

Table 8.3-1 below provides a description of the Trouble Ticket HTML Submit Screen fields.

Table 8.3-1. Trouble Ticket HTML Submit Screen Field Description

Field Name	Data Type	Size	Entry	Description
ID	character	30	System generated	Submitter Id
Name	character	30	System generated	Submitter Name
E-mail address	character	64	System generated	Submitter E-mail Address
Phone	character	30	System generated	Submitter Phone Number
Home DAAC	character	60	System generated	Submitter Home DAAC
Impact	selection	4	Required	Impact to Submitter
Short description	character	125	Required	Short description of problem
Detailed problem description	character	245	Optional	Long description of problem

When the information is completed, the user can submit the Trouble Ticket by clicking on the **Submit** button on the lower half of the screen. (The Success screen appears when a Trouble Ticket is successfully submitted. See Section 8.3.2 below.) The Problem Information Fields can be cleared by clicking on the **Reset** button. The user also has the choice of returning to the Trouble Ticketing Homepage or going to the Trouble Ticket Help screen by clicking on the respective icons at the bottom of the page.

8.3.2 ECS Trouble Ticketing HTML Success Screen

The HTML Trouble Ticket Success screen indicates a successful submission and reports the Trouble Ticket Id.

From this screen, the user is provided with the following information/options:

- Confirmation that the trouble ticket was successfully submitted, the trouble ticket identification number, and who submitted the trouble ticket.
- Notification that an E-mail message has been sent to the user indicating that a Trouble Ticket has been submitted and when it was closed. Selecting [this Trouble Ticket](#) will open the Trouble Ticket Detailed Screen.
- Instructions telling the user how to check the progress of Trouble Ticket resolution.

The user also has the choice of returning to the Trouble Ticketing Homepage or going to the Trouble Ticket Help screen by clicking on the respective icons at the bottom of the page.

8.3.3 ECS Trouble Ticketing HTML List Screen

The HTML Trouble Ticket List screen is used by registered ECS users to List Trouble Tickets for a user and links the listed Trouble Ticket Number to the Trouble Ticket Detailed Screen.

Table 8.3-2 below provides a description of the Trouble Ticket HTML List Screen fields.

Table 8.3-2. Trouble Ticket HTML List Screen Field Description

Field Name	Data Type	Size	Entry	Description
Trouble Ticket Number	character	15	System generated	Trouble Ticket Id
Problem Short Description	character	125	System generated	Short Description of Problem
Status	character	20	System generated	Status of Trouble Ticket

The user also has the choice of returning to the Trouble Ticketing Homepage or going to the Trouble Ticket Help screen by clicking on the respective icons at the bottom of the page.

8.3.4 ECS Trouble Ticketing HTML Detailed Screen

The HTML Trouble Ticket Detailed screen is used by registered ECS users to see a more detailed output of a Trouble Ticket.

Table 8.3-3 below provides a description of the Trouble Ticket HTML Detailed Screen fields.

Table 8.3-3 Trouble Ticket HTML Detailed Screen Field Description

Field Name	Data Type	Size	Entry	Description
ID	character	30	System generated	Submitter Id
Name	character	30	System generated	Submitter Name
E-mail address	character	64	System generated	Submitter E-mail Address
Phone	character	30	System generated	Submitter Phone Number
Home DAAC	character	60	System generated	Submitter Home DAAC
Status	selection	4	System generated	Status of Trouble Ticket
Impact	selection	4	System generated	Impact to Submitter (low, medium, high)
Short description	character	125	System generated	Short description of problem
Detailed problem description	character	245	System generated	Long description of problem
Log	character	unlim.	System generated	Diary of problem resolution

The user also has the choice of returning to the Trouble Ticketing Homepage or going to the Trouble Ticket Help screen by clicking on the respective icons at the bottom of the page.

8.3.5 ECS Trouble Ticketing HTML Help Screen

The HTML Trouble Ticket Help screen is used by registered ECS users to get help with the HTML screens.

This screen provides general information on the following:

- _ Index -- links that scroll the screen to the Introduction, Submit Page, and List Page sections listed below.
- _ Introduction – provides information about the Trouble Ticket Help page
- _ Menu Page – describes the Trouble Ticketing Menu page.
- _ Submit Page – describes the Trouble Ticket Submit page.
- _ Success Page – describes the Trouble Ticket Success page.
- _ List Page – describes the Trouble Ticket List page.
- _ Detailed Page - describes the Trouble Ticket Detailed page.

8.4 Emergency Fixes

Any emergency may be dealt with on an ad hoc basis, but contingency plans, contact points for supervisors, responsible engineers, Sustaining Engineering Organization, vendors, and general guidelines need to be in place to provide a common framework for emergency response to crisis-level situations. Emergency fixes may have already been implemented on a temporary basis by the Trouble Ticket Review Board with concurrence from the CCB Chair who later receives the CCR to document/implement the permanent change. Urgent items will be reviewed by the next CCB meeting.